

車内ユーザへの通信リソース提供のための動的ネットワーク融合方式

今井 尚樹

堀内 浩規

(株) KDDI 研究所

1. はじめに

身の回りに多くのネットワーク接続端末が存在するユビキタス通信環境では、人と車をシームレスに接続することで快適・便利な ITS 社会を実現することが期待されている。例えば、タクシー等の車内に乗り込むユーザがアプリケーションを実行する場合、携帯電話機の画面よりも後部座席のモニターを利用することで、より満足度の高いアプリケーション実行環境とすることが可能となる。本稿では、このようにユーザ持込み端末・ネットワークと、車内端末・ネットワークを連携可能とするため、ITS を対象としたネットワーク同士の融合方式について示す(図1参照)。



図1: ネットワークの融合

2. 要求項目

移動するユーザが、ネットワークに持込み端末を接続する一般的なシナリオ例としては、ホットスポットにおける接続や、ホーム/オフィスネットワークへの接続が考えられる。ホットスポットでは、不特定多数のサービス利用者に対してネットワークあるいはプリンタ等の機器を利用可能とし、ホーム/オフィスネットワークでは、予め定められたユーザに対してネットワーク接続環境を提供する。その一方で、1. に示したような想定シナリオでは、以下のような要求項目が挙げられる、

[要求1] 車内のユーザのみが接続可能であること

車内ネットワークに対して、乗車中のユーザ以外の歩行者ユーザや併走する車内のユーザなど、意図しないユーザが接続できないことが要求される。

[要求2] 降車したユーザが車内ネットワークに接続できないこと

降車したユーザを含む、車両から離れたユーザが、車内端末・ネットワークを占有し続けたり、以前の接続情報を使用して接続できないことが要求される。

[要求3] 矛盾なく IP アドレスを割り当てられること

ユーザの持込み端末と融合先となる車内ネットワークの端末間で、IP アドレスを重複することなく割り当てられることが要求される。

要求1を満たすためには、従来のホットスポットよりも狭い概念でサービス提供場所を絞り込む必要がある。このためには、ユーザ端末側で無線レベルでの信号受信をトリガとする手法の適用は困難であり、車内でのみ接続情報を取得可能とするための手法が必要となる(3.2.1で後述)。

要求2を満たすためには、融合ごとに無線設定やネットワーク設定を変更するとともに、ユーザが車両から離れたことを車内ネットワークが認識し、車内ネットワーク主導でネットワークの分離動作を実行できなければならない。

要求3を満たすためには、重複のないアドレス割当てに加えて、割当てた IP アドレスやその他ネットワーク設定情報をユーザ端末に通知するための手法が必要となる。

次章では、これらのアプローチにもとづく動的ネットワーク融合方式を述べる

3. 動的ネットワーク融合方式

3.1. 融合前のネットワーク

ネットワーク融合動作が開始される前、ユーザネットワークと車内ネットワークは完全に独立しており、それぞれネットワーク的に接続されていない状態である。

3.1.1. ユーザネットワーク

ユーザが車両に乗車する前のユーザネットワークは、1台のユーザゲートウェイと、任意の台数のユーザクライアントから構成される。ユーザクライアントはユーザゲートウェイの配下に位置し、ユーザゲートウェイを経由して外部ネットワークに接続する。例えば、ユーザが携帯電話機、PC、その他身の回りのネットワーク接続可能な機器を持っているとき、携帯電話機がユーザゲートウェイであり、その他の端末がユーザクライアントとなる。また、ユーザが携帯電話のみを使用する場合、ユーザゲートウェイは存在しない。

定常状態において、ユーザクライアントの IP アドレスはユーザ

ゲートウェイから割当てられる。これにより、ユーザゲートウェイは配下のユーザクライアントの台数および IP アドレスを把握する。なお、IP アドレスを割当てるとき、ユーザゲートウェイのアドレス割当て機能は DHCP[1]により実現可能である。

また、ユーザゲートウェイと各ユーザクライアントが無線インタフェースで接続される場合、無線区間は暗号化によりセキュア化されることを前提とする。例えば、WEP、TKIP、WPA 等によりユーザゲートウェイとユーザクライアント間のパケットが暗号化されているものとする。

3.1.2. 車内ネットワーク

融合前の車内ネットワークは、1台の車内ゲートウェイと、任意の台数の車内クライアントから構成される。車内クライアントは車内ゲートウェイの配下に位置し、車内ゲートウェイを経由して外部ネットワークに接続する。車内ゲートウェイとしてはカーナビを含む車載機、車内クライアントとしては後部座席のディスプレイモニタ等が考えられる。

定常状態においては、ユーザネットワークと同様に、車内クライアントのアドレスは車内ゲートウェイから割当てられる。一方で、車内ゲートウェイはネットワーク上の管理サーバに対して外部ネットワーク経由で定期的に状態登録を行う。状態登録のための車内ゲートウェイと管理サーバ間の通信チャネルは、任意の手法により暗号化が施される。管理サーバに登録される情報としては、車両に予め割当てられた車両に固有の ID、車内ゲートウェイの外部インタフェース側に割当てられた IP アドレス、サービス提供中/スタンバイ中/サービス停止中といったサービスステータス状態が挙げられる。

スタンバイ中の車内ネットワークは、無線区間の暗号化や無線電波の停止により、外部から接続されないようにする。

3.2. ネットワークの融合

ネットワーク融合処理は、車両に乗車したユーザによるユーザゲートウェイでの融合開始処理(融合開始処理フェーズ)、ユーザゲートウェイによる融合要求送信から管理サーバによる処理(融合要求通知フェーズ)、ユーザネットワークと車内ネットワークにおける設定変更処理(融合設定変更フェーズ)に分類される。

3.2.1. 融合開始処理フェーズ

ユーザゲートウェイが管理サーバにアクセスするためには、管理サーバの情報や乗車している車両の車両 ID をユーザゲートウェイに通知しなければならない。ここでは実現手段として2つの例を挙げる。

[例1] USB セキュアキーの使用

証明書を含むサーバ情報や車両 ID を含む USB セキュアキーを車内座席等に設置しておく手法である。ユーザゲートウェイが PC 等の USB インタフェースを持つ端末である場合、USB セキュアキーを挿入することで、管理サーバへの接続が自動的に開始される。

[例2] 2次元バーコードの使用

後部座席のディスプレイに接続情報を含む2次元バーコードを描画する。ユーザゲートウェイが携帯電話機の場合、カメラからこのバーコードを読み取り、携帯電話機内のソフトウェアが保持するセキュア情報と組み合わせる上で管理サーバと通信する。

3.2.2. 融合要求通知フェーズ

要求通知フェーズの動作シーケンスを図2に示す。

ユーザゲートウェイは、管理サーバとの間でセキュアなパスを構築する(図2(1))。ユーザゲートウェイは管理サーバに対して、ネットワーク融合要求を送信する(図2(2))。

このネットワーク融合要求にて、ユーザゲートウェイは割当て要求する IP アドレスの個数に加えて、割当て方式についても管理サーバに要求する。例えば、ユーザゲートウェイは要求する IP アドレスの個数のみを通知することで、任意の IP アドレスの割当てを要求可能である。一方で、割当て IP アドレスについて具体的な

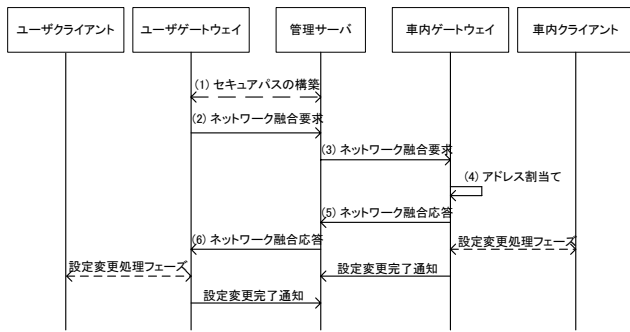


図 2：ネットワーク融合時の動作シーケンス

希望がある場合、希望する IP アドレスを明示して管理サーバに通知する。

ユーザゲートウェイからネットワーク融合要求を受信した管理サーバは、車両 ID をキーとして当該車内ゲートウェイのサービスステータスを検索する。状態がスタンバイであれば、外部ネットワークアドレスに対してネットワーク融合要求を通知する(図 2(3))。

車内ゲートウェイは、ネットワーク融合要求に含まれる IP アドレス割当て要求を見て、アドレスの割当てを行う(図 2(4))。ユーザゲートウェイが要求する IP アドレス群を割当て可能である場合、車内ゲートウェイは車内ゲートウェイの内部インタフェース IP アドレスと車内クライアントの IP アドレスを、ユーザネットワーク側の設定と合わせる。一方で、ユーザゲートウェイが任意の IP アドレス群の割当てを要求する場合、車内ゲートウェイはユーザゲートウェイが要求する台数の割当てができればよい。

車内ゲートウェイは管理サーバに対して、融合ネットワークが使用する無線情報(無線チャネル、セキュリティ情報等)と、ネットワーク情報(ユーザゲートウェイ、ユーザクライアントに割当てする IP アドレス、車内ゲートウェイの内部ネットワーク IP アドレス等)をネットワーク融合応答として通知する(図 2(5))。

管理サーバは、車内ゲートウェイから受信したネットワーク融合応答をユーザゲートウェイに対して転送する(図 2(6))。

3.2.3. 融合設定変更フェーズ

車内ゲートウェイとユーザゲートウェイは、融合要求通知フェーズで決定した設定情報を、ブロードキャストによりそれぞれの配下のクライアントに対して通知する。融合ネットワークの情報を受信したクライアントは、送信元となるゲートウェイに対して ACK パケットを送信する。配下の全クライアントから ACK パケットを受信すると、ゲートウェイは設定変更要求をブロードキャストする。ゲートウェイおよび設定変更要求を受信したクライアントは融合ネットワーク用の無線設定、ネットワーク設定に実際に変更する。双方のゲートウェイは、管理サーバに対して設定変更完了通知を送信し、ネットワークの融合が完了する。

融合後、ユーザゲートウェイと車内ゲートウェイは融合ネットワークに対して定期的にブロードキャストによりビーコンパケットを送信する。

3.3. ネットワークの分離

ネットワークの分離動作が開始されるトリガには、明示的なユーザの意思のみならず、ユーザ端末が車内から離れたと推測される場合も含まなければならない。すなわち、ネットワークの分離は、①ユーザゲートウェイからネットワーク分離要求パケットが送信される場合、②ユーザゲートウェイが融合ネットワーク内に定期的にブロードキャストするビーコンパケットを、車内ゲートウェイが一定回数以上受信しない場合、③ネットワーク管理上の理由により車内ゲートウェイがネットワークの分離を要求する場合、に実施される。

上記①の場合の動作シーケンスを図 3 に示す。ユーザゲートウェイは初めに車内ゲートウェイに対してネットワーク分離要求を送信する(図 3(1))。ネットワーク分離要求を受信した車内ゲートウェイと、車内ゲートウェイからの ACK を受信したユーザゲートウェイは(図 3(2))、それぞれのクライアント端末に対してネットワーク分離動作を開始する。

ユーザネットワークおよび車内ネットワークの分離動作では、各ゲートウェイが融合時と同様の手法を用いて、ネットワーク分離動作をクライアントに通知し、自らも融合前のネットワーク状態に戻る(図 3(3))。ただし、無線設定やネットワーク設定は、ゲートウェイクライアント間で明示的には通知されず、各端末に保持された情報を利用して融合前の状態に戻す。双方のゲートウェイは、管理サーバに対して分離完了を通知し分離動作が完了する。

なお、②や③の場合は、上記のうち車内ネットワーク側のみの

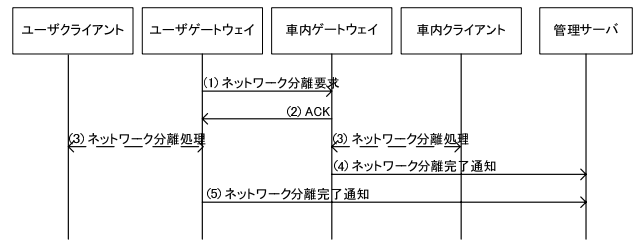


図 3：ネットワーク分離時の動作シーケンス

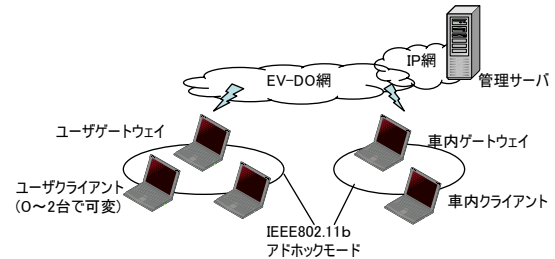


図 4：システム構成

処理となる。しかしながら、ユーザゲートウェイも車内ゲートウェイからの定期的なビーコンを受信しなくなることでタイムアウトが発生するため、ユーザネットワークも初期状態に戻ることができる。

4. 動的ネットワーク融合方式の実装と動作試験

4.1. 実装システム

3. に示した動的ネットワーク融合方式を、Linux OS 搭載の PC 上で実装した。実装システムの構成図を図 4 に示す。ユーザゲートウェイおよび車内ゲートウェイは、IEEE802.11b と CDMA2000 1x EV-DO の 2 種類の通信インタフェースで通信可能である。各ゲートウェイと外部ネットワーク間の通信には EV-DO を、各ゲートウェイと配下の各クライアント間の通信には IEEE802.11b を使用する。なお、今回の実装では IEEE802.11b のアドホックモードを使用した。

4.2. 動作試験

提案方式の実装システムの動作試験を行った。ユーザクライアント数を 0 台~2 台で変化させて融合および分離の時間を測定した。車内クライアントの数は 1 台とした。それぞれ 10 回ずつ融合と分離を繰り返し、平均時間を計算した。表 1 に結果を示す。融合時間はユーザゲートウェイがネットワーク融合要求送信後から、設定変更完了通知が管理サーバに到達するまでの時間とした。また、分離時間は、ユーザゲートウェイが車内ネットワークに対してネットワーク分離要求を送信してから、ネットワーク分離完了通知が管理サーバに到達するまでの時間とした。

ユーザクライアントの台数が 0 台の場合、ユーザゲートウェイとユーザクライアント間での設定変更通知が不要となるため、ユーザクライアント数が 1 台以上の場合と比較して、約 180ms~200ms 融合および分離時間が短くなった。ユーザクライアントが 1 台の場合と 2 台の場合ではほとんど差が見られたかった。ユーザクライアント数を大きく増加させた場合、設定変更フェーズにおける ACK パケットの衝突発生も予想されるが、現時点でユーザが保持するユーザクライアント端末数は数台程度と予想されるため問題にはならないと考えられる。

表 1：測定結果

ユーザクライアントの台数[台]	融合時間[s]	分離時間[s]
0	1.13	0.32
1	1.31	0.50
2	1.33	0.50

5. おわりに

本稿では、ITS における人と車のシームレス通信を実現するための動的ネットワーク融合方式を示した。最後に、日頃ご指導頂く(株)KDDI 研究所秋葉所長および鈴木執行役員に感謝する。本研究の一部は NICT からの受託研究「ユビキタス ITS の研究開発」の成果である

参考文献

[1] R. Droms, "Dynamic Host Configuration Protocol," IETF RFC2131, March 1997.