Vol.2016-CSEC-73 No.11
Vol.2016-IOT-33 No.11
2016/5/26

Wi-Fi モバイルルータにおける 位置トレーサビリティの検討と対策

中村 暢宏[1,a)]　上原 哲太郎[1,b)]

概要：モバイルコンピューティングが進展するなか，個人のプライバシを守ることは重要な課題とされている．Wi-Fi においては，端末を一意に識別できる MAC アドレスが外部から観測できることから，MAC アドレスを用いて端末のユーザを許可なく追跡されうる問題が知られている．この問題に対しては，クライアント端末においては MAC アドレスを定期変更し，使い捨てることが有効であることが知られている．本研究では，これまで深く議論されてこなかったモバイルルータに焦点を当て，常時稼働するモバイルルータに対して有効な位置プライバシ対策がないことを明らかにし，新たな対策を提案した．

Nobuhiro Nakamura[1,a)]　Tetsutaro Uehara[1,b)]

1. はじめに

現代社会においてコンピュータの活躍する場面が増えるに従い，データ化される個人情報を不本意な漏洩や悪用から守ることは人々にとって大きな関心事となっている．本研究では，そのうち人々の位置に関する情報に焦点をあてる．Wi-Fi[*1] には，端末に固有の識別子である MAC アドレスに起因した位置プライバシ問題があることが知られている．

この問題の対策についてはすでに多く研究が行われ，部分的な対策は市販のクライアント端末にも実装されており，実用の段階に入っていると考えられる．しかしながら，モバイルルータを用いるシナリオにおける問題は過去に研究例が少なく，実用的な対策は検討されてこなかった．そこで，本研究では特に Wi-Fi のモバイルルータとそれに接続するクライアント端末に着目し，位置プライバシの問題及びその対策について検討する．

本研究では，位置プライバシ問題に対して実用的なリスク低減策を開発することを目的とする．加えて，ユーザにとっての便益の観点から，開発する対策は以下のような特徴を備えているべきであるとしている．

- 802.11 規格を変更しなくても，ベンダ間の運用互換性の問題を起こしにくいこと
- リスクの低減に際して，ユーザの自発的な行動を要求しないこと
- 適用前と同等のユーザエクスペリエンスを担保すること

こうした要件を満たすことによって，対策を取り入れるにあたっての障壁が少なくなり，より多くのユーザが使える対策が実現されると考えられる．

まず，Wi-Fi の MAC アドレスにまつわる位置プライバシ問題と過去の研究における対策を紹介する．その上で，モバイルルータにおける課題をまとめる．本論では，最後にモバイルルータとモバイルルータに接続するクライアント端末においてより適切な手法を提案し，その実装について議論する．

2. 背景

2.1 インターネット接続と Wi-Fi

携帯電話回線の高速化・大容量化によって，携帯電話は場所を問わず高速なインターネット接続が行えるようになった．このため，近年のアプリケーションは，インターネットへの常時接続を前提とする機能を備えることが多くなっている．例えば，SNS 上の更新が直ちにユーザのスマートフォンにプッシュ通知されるといった機能は珍しくない．このようにして，スマートフォンはユーザが直接使

[1] 立命館大学大学院情報理工学研究科情報理工学専攻
[2] 立命館大学情報理工学部情報システム学科
[a)] n.nakamura@cysec.cs.ritsumei.ac.jp
[b)] uehara@cs.ritsumei.ac.jp

[*1] Wi-Fi Alliance (`http://wi-fi.org/`) の登録商標である．本来は Wi-Fi Alliance が認定する技術を指す語であるが，本論では IEEE 802.11 規格 [1]（以下，802.11 規格という）に則る無線 LAN の技術を総称して言う．

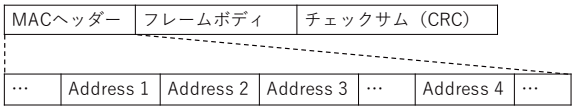

図 1 Wi-Fi の MAC フレームとアドレスフィールド

表 1 図 2 においてクライアント端末から WAN に向かう Wi-Fi フレームのアドレスフィールド

フィールド	内容の指す端末
Address 1	AP（Receiver，BSSID）
Address 2	クライアント端末（Source かつ Transmitter）
Address 3	AP 端末に内蔵のゲートウェイ（Destination）
Address 4	なし

用していない時にも通信を行うことで，その利便性を向上させてきた．

そのような携帯電話回線の利便性を，専用の装備のない端末にも享受させる仕組みの一つとしてモバイルルータがある．例えば，多くのスマートフォンはその携帯電話回線を他の端末と共有するために AP として機能させる（テザリング）ことができる．こうすることによって，任意の Wi-Fi クライアント端末を場所を問わずインターネットに接続させることができる．このほか，主に外出時にクライアント端末を Wi-Fi を通じてインターネットに接続させるための専用端末（モバイルルータ）が市販されている．本論では，テザリングを行うスマートフォンなどの端末とモバイル AP 専用端末を総称してモバイルルータと呼ぶことにする．

2.2 MAC アドレスに係る位置プライバシ問題

Wi-Fi において，端末に付与された MAC アドレスは，その電波通信を傍受することによって容易に観測できる．このことが，位置プライバシ問題となることが知られている．以下の小節では，まず Wi-Fi における MAC アドレスの使われ方について解説し，その上で位置プライバシ問題を議論する．

2.2.1 Wi-Fi と MAC アドレス

Wi-Fi における MAC アドレスの用途は，大きく次の二つに分かれる．

- フレームの伝送先を制御する
- 暗号化鍵や完全性符号の生成に用いる

本節では，このうちの前者について解説を行う．

Wi-Fi におけるフレームは**図 1** に示す通り，種類を問わず共通の MAC ヘッダーを持っている．この MAC ヘッダーの各アドレスフィールド (Address 1-4) に MAC アドレスを記すことによって，フレームの伝送先が制御される．

図 2 にモバイルルータとクライアント端末が作るネットワークを示した．

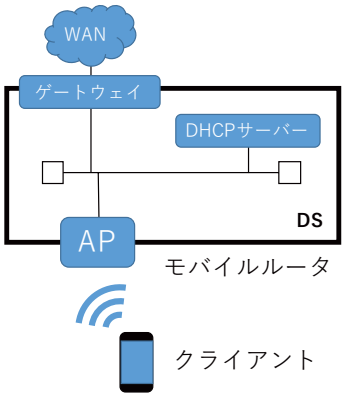

図 2 Wi-Fi モバイルルータとクライアント端末からなるネットワークの構成

表 2 To DS と From DS の値と Address 3 の意味の対応

To DS	From DS	Address 3 の意味
0	0	なし
1	0	Destination
0	1	Source

図 2 の四角く囲った部分を DS[*2] という．AP は，無線媒体と DS の間でフレームを中継する役割を持つ．一つの AP がクライアント端末に提供するサービスを BSS[*3] といい，AP の MAC アドレスを BSSID という．このネットワークにおいて，クライアント端末が WAN に向けてフレームを送信する例を用いて各アドレスフィールドの意味を説明する．

この例でクライアント端末が送出するフレームのアドレスフィールドは**表 1** のようになる．Wi-Fi においてフレームの伝送制御に用いられる MAC アドレスとして，イーサネットと同様の Destination と Source に加えて，Receiver と Transmitter が存在する．Address 1 と Address 2 はそれぞれ，無線で送られるフレームの Receiver と Transmitter である．

MAC ヘッダーの別の箇所には To DS と From DS というフラグが存在し，これらによって Address 3 及び Address 4 の意味が決定される．To DS はフレームが DS 内のデバイスに宛てられたものかどうかを表す．そうである場合は 1，そうでない場合は 0 である．From DS は同様にフレームが DS 内のデバイスから送られたものであることを表す．To DS，From DS の値と Address 3 の意味の対応は**表 2** のようになる．Address 4 は To DS = 1，From DS = 1 の場合にのみ使用されるが，これは Wi-Fi を用いてメッシュネットワークを構成する場合に限られる．

例の場合では，To DS=1, From DS=0 となる．この例のフレームを受け取った AP は，To DS フラグを確認し，Destination である DS 内のゲートウェイにフレームを転

*2 distribution system
*3 basic service set

送する．

このように，MAC アドレスは Wi-Fi の MAC ヘッダーを通じて平文で記され，無線でやり取りされる．Wi-Fi は通信を暗号化する仕組みを持っているが，これによって暗号化される部分は MAC フレーム中のフレームボディに限られる．暗号化を施していても DS 内に設置されるゲートウェイや DHCP サーバといった端末の MAC アドレスは依然として平文でやり取りされる点に注意を要する．

2.2.2 Wi-Fi と位置プライバシ問題

製品の利用状況や個人の行動状況といった個人情報は，ターゲット広告やサービスの改善に有用である．技術の進歩が個人の行動をより多くトレース可能にしてきた．しかしながら，他人に行動をより詳細に把握されることはより多くの人が不快に感じる．どの個人情報が他人に知られたくないか，あるいはある個人情報を他人に提供することが利益になるかどうかはユーザの主観であり，画一的な基準は存在しない．より幅広いユーザのプライバシ観に応えるため，個人情報の収集にあたっては当人の同意を得ること，つまり個人情報の提供を当人が選択できることが重要であると考えられる．この「自己の情報を他人に知らせるかどうかを当人の意思で決める」ことは今日における情報プライバシ権の捉え方の一つである [2]．収集した個人情報の利用目的やプライバシポリシーの明示は，こうした個人の判断材料としてプライバシの向上に資すると考えられる．

Wi-Fi において通信を傍受できるのは狭い範囲に限られるため，ある MAC アドレスをこの方法で観測することは，そのアドレスが付与された端末が観測者の近くに存在することを意味する．攻撃者は，複数の箇所で通信を傍受しながら観測できる MAC アドレスを収集することによって，各 MAC アドレスに対応する端末がどの地点に存在するか，あるいは存在したかをトレースことができる．このような記録はユーザの行動や属性に関連するものであり，個人にとって機微な情報となりうる．

Wi-Fi の電波を用いた位置トレースは，当人の同意を得ることなく，また当人に気づかれずに行うことができる．こんにち，さまざまな企業が位置情報サービスのために Wi-Fi の AP の識別子と位置の情報を収集している．こうして収集された情報がサービスを通して公開された場合，例えば SNS 上に誤って公開した SSID や MAC アドレスから住所が特定されるなどの問題 [3] が発生しうる．そのため，こうした企業は情報収集を拒否するための仕組みを人々に提供している．しかし，そういった仕組みの多くはオプトアウト型，すなわち情報収集を拒否するために人々の自発的な行動が要求されるものである．しかしながら，Wi-Fi の位置情報収集を行う企業は通常，情報収集の事実を人々に確実に伝える手段を持たない．したがって，人々が情報収集を拒否する機会が必ず与えられるとはいえず，プライバシ問題であると考えられる．

ここで挙げた例は，据え置きの AP に関する情報収集であるが，同様の情報収集はモバイル端末に対しても行われうる．さらに，こうした情報収集が悪意ある者によって行われる場合があり，同意のない情報収集を難しくする対策は悪意ある攻撃を抑止するためにも重要であると考えられている．

2.3 MAC アドレスの定期変更による対策

前節で述べたような問題に対しては，古くから MAC アドレスを定期的に変更するような対策が議論されてきた [4]．MAC アドレスを変更することで，攻撃者は同じ端末の追跡を続けることが難しくなる．MAC アドレスは前述のとおり，フレームの制御などに用いられ，変更されることが想定されていない．このことから，これまでに議論されたいくつかの対策は 802.11 規格の変更，あるいは新たなプロトコルの導入 [5], [6] を前提とするものである．しかし，2016 年 4 月現在に位置プライバシの保護を目的とした IEEE 802.11 規格の変更を議論するタスクグループは存在せず，そのような手法による対策は近い将来には実現しないと考えられる．

そのような中，近年では実用的に通信が保てる範囲で MAC アドレスを更新するような対策が議論されてきた．クライアント端末においては

- AP との接続するとき
- AP を探索するとき

においてランダムな MAC アドレスを新たに生成して用いても通信上の問題は少ないと考えられる．しかしながら，MAC アドレスの同一性を持って認証の代わりとするネットワークが存在するなどの実用上の課題があり，ネットワーク毎に MAC アドレスのランダム化をオプトアウトできるようにするといった工夫が必要である．

このように可能な範囲でクライアント端末の MAC アドレスを変更する手法は，いくつかの一般に利用出来る製品で実装されているほか，近年の IEEE と IETF[*4] の会合において継続的に試験運用が実施されてきた [7]．

2.4 変更前後の MAC アドレスの関連付け

定期的な MAC アドレス変更には，過去の研究において，周囲の観測者が変更前後の MAC アドレスを容易に関連付けできる問題が指摘されてきた．MAC アドレスが変わっても端末は同じ場所に存在するため，電波中の通信を観察すると違う MAC アドレスの持ち主が同じ端末であることを攻撃者は推測することができる．この問題に対して，過去の研究では MAC アドレスの変更前後に通信を一切行わない Silent Period[8], [9] を設けることによって攻撃者による追跡を撹乱する手法が議論されてきた．

[*4] Internet Engineering Task Force

ただし，これは MAC アドレスを変更する段階を攻撃者に観測されることを前提にした問題であり，この前提は長期に渡る位置トレースを考える上で現実味が薄い．

前節で述べた通り，一部のアプリケーションはインターネットとの常時接続を期待した機能を備えており，Silent Period による対策は行われるべき通信を阻害する可能性がある．

3. モバイルルータにおける問題

前節までに触れた問題は，据え置きの AP を利用するモバイルクライアント端末についてのものであった．本節ではモバイルルータとそれに接続するクライアント端末に焦点を移して議論を始める．

まず，据え置きの AP とモバイルルータについて，AP 自体とそれぞれに接続するクライアント端末の置かれる状況の違いを整理する．モバイルルータは文字どおり移動できる AP であり，特に通信しながら移動できる点で据え置きの AP とは大きく異なる．モバイルルータに接続する場合では，クライアント端末の移動にまつわる制約が少ない．

さて，前節で述べた対策は据え置きの AP に接続するクライアントに対するものであったが，これをモバイルルータの場合に当てはめた手法について検討する．具体的には，モバイルルータが AP をサービスしていない状態で（あるいはサービスを中断して）BSSID を切り替えるような手法を考える．

前述の通り，モバイル端末においてもインターネットとの常時接続が期待されるようになっており，クライアントが一つも接続していない状態が続いている場合など明らかな場合を除いて，AP がユーザの明示的了解なしにサービスを中断することはユーザエクスペリエンスを損ねる可能性がある．

サービスを中断するにあたって，ユーザの同意を得るような手法を考えることができる．しかし，AP は一般的にユーザと対話する手段あるいはプロトコルを持っていないため，本論で決めた制約に適う実装は困難である．

このことは，モバイルルータが移動しながら長時間同じ MAC アドレスを使い続ける可能性を示唆している．モバイルルータによって家庭の固定回線を代替しているケースを例に考える．つまり，家庭内でも外出時にもモバイルルータを利用しているというケースである．

以上のことから，ユーザの使い方によって，モバイルルータの電源を入れる際に BSSID をランダムなものに変える手法では，同じアドレスを長時間使うことになり，位置トレースリスクの低減が限定的となりうることがわかる．

また，Wi-Fi の AP には MAC アドレスに加えて，SSID[*5] と言う識別子が付いている．SSID は文字列であり，ユーザやクライアント端末が AP を見つけるために使用する．ユーザは最大 32 バイト長の任意の ASCII もしくは UTF-8 の文字列を SSID に設定できる．SSID も MAC アドレスと同様に無線媒体を通じて外部から観測でき，端末の位置トレースに利用されうる．

この SSID による問題は，[10] に示される手法で SSID をランダム化することが対策となりうる．しかしこの手法では，802.11 規格を変更する必要はないが，フレームにベンダ独自の拡張を加えなければならず，ベンダ間の互換性に課題が残る．

4. 対策の検討

本研究では，これまでに議論したモバイルルータにおける問題に対して，802.11 規格を変更することなく対策することを考える．そうすることの利点は，802.11 規格を定める委員会での議論が省け，早期に実現が可能であると考えられることである．本論では，モバイルルータにおいて MAC アドレスの定期変更を実現するため，クライアントとの通信を維持しつつモバイルルータの持つ MAC アドレスを変更する手法を検討する．

まず，手法の概要を**図 3** に示す．本手法は，以下の 3 要素からなる．

- モバイルルータの AP に接続するクライアントに定期的に別の新しい AP に移行させることによって BSSID の定期変更を実現する．
- クライアント端末の MAC アドレスは，AP を移行しながらモバイルルータを利用している間は一貫したものを使い，ユーザが端末を利用していない時間に接続を切断して MAC アドレスを切り替える．
- DS 内デバイスの MAC アドレスは，各モバイルルータで共通のものを用いることによって，匿名化する．

これらの要素を組み合わせることによって，ユーザとともに移動するモバイルルータとそのクライアント端末を長期にわたって追跡することをより困難にする．以下に続く小節ではそれぞれの要素についてその実装方法を議論する．

4.1 定期的な AP の移行

本手法では，モバイルルータに一時的に二つ目の BSS を生成させ，クライアントに新しい BSS へ移行させることによって，ルータの BSSID を変更する．本手法による BSSID 変更の流れを以下に示す．

(1) モバイルルータが AP を一つだけ運用しているとする．この AP を AP_k という．
(2) AP_k とは別の AP，AP_{k+1} をモバイルルータが立ち上げる．AP_{k+1} にはランダムに新たな BSSID を割り当てる．
(3) AP_k から各クライアントに AP_{k+1} への移行を勧告する．

[*5] service set identifier

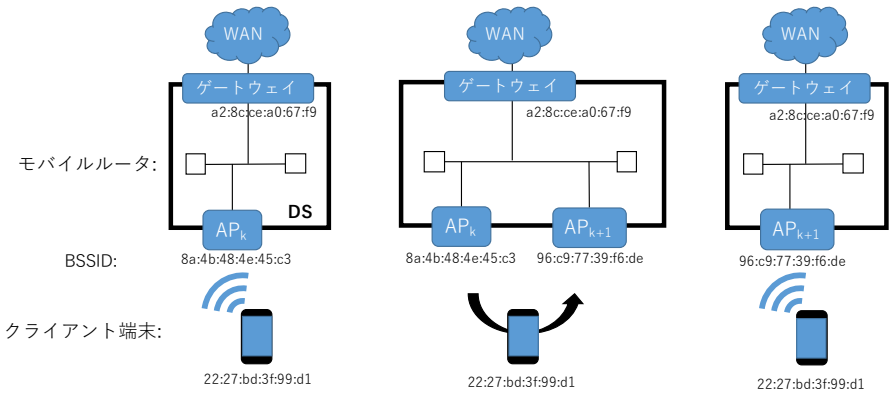

図 3 定期的に AP を移行することによる BSSID の変更

(4) 各クライアントが AP_{k+1} へ移行するのを待つ．
(5) AP_k の運用を終了する．
モバイルルータはこれを繰り返すことで BSSID の定期変更を実現することができる．無線媒体を監視している攻撃者は，同じ端末の MAC アドレスを容易に関連づけることができるが，移動する同じ端末の通信を全て監視することは困難であると考えられる．よって，同じ端末の追跡は一般に追跡する時間が長くなるほど難しくなると考えられる．

この利点は，通信への影響が少なくて済み，ユーザの同意が不要であると考えられることである．BSSID を変更しても，レイヤー 3 以上で通信の当事者となる端末の MAC アドレスは変わらないため，それらのセッション等に影響はないと考えられる．但し，BSS を移行する間は一時的に通信が不通にとなり，フレームロストが起こる場合がある．AP 間の移行に高速 BSS 移行 [*6] を用いることによって通信が不通となる時間を減らすことができる．

クライアント端末に AP の移行をさせる勧告は，802.11 規格に定められている BSS 移行管理 [*7] の機構を用いる．BSS 移行管理では，ロードバランシングやサービスの終了といった理由で，AP に接続しているクライアントに対して他の BSS に移行することを促す．これに際して，AP は移行先候補となる近隣の AP の情報を BSS 移行管理リクエストとしてクライアントに伝える．さらに，AP は同じリクエストを用いて，サービスが終了するまでの時間と，クライアントが AP からすぐに切断されるという旨を通知することができる．

これを受けたクライアントは，移行を行うかどうかを決定してその旨を AP に返答する．返答に用いるステータスコードとして，移行を拒否するものも規格に示されており，どのような返答を行うかは規定されていない．しかしながら，AP からクライアント端末へサービスの終了を予告するため，ユーザにとっての利益を考えれば，できれば移行を許諾するようクライアント側のプログラムを組むことは比較的合理性が高い．

本研究では，勧告によってクライアントを決まった AP に移行させることの実現性を実験によって調べた．その報告は続く小節で述べる．また，提案手法では必須とはしていないが，高速 BSS 移行の仕組みでは MAC アドレスや SSID とは別の識別子を外部に露出することを AP に求めている問題が存在する．これについても別の小節で議論する．

4.1.1 検証実験

提案手法においては AP の求めによってクライアント端末に BSS を移行させる必要がある．802.11 規格において，BSS 移行管理リクエストを受信したクライアント端末が移行を実施するかどうかは未規定である．その実現性を検証するため，接続しているクライアントを新しい BSS に移行を促すシステムを構築した．その上で，BSS 移行管理に対応するデバイスを接続させ，その動作を確かめた．

4.1.1.1 準備

システムの構築には，Linux 向けの AP 構築ツールである hostapd[*8] と新たに作成した Python スクリプトを用いた．構築したシステムを実験システムという．実験に使用した主なソフトウェアのバージョンは**表 3** に示すとおりである．

実験システムは，以下のように振る舞う．
(1) 新しい AP を立ち上げる．これを AP_1 と呼ぶ．
(2) 30 秒待つ．
(3) 新しい AP を立ち上げる．これを AP_2 と呼ぶ．
(4) AP_1 に接続しているクライアントに対して，AP_2 への移行を勧告する BSS 移行管理リクエストを送信する．
(5) 10 秒待つ．
(6) AP_1 に接続しているクライアントの数が 0 であれば (4) へジャンプする．
(7) AP_1 の運用を中止する．
なお，実験システムは AP 間で高速 BSS 移行が行えるよう

[*6] Fast BSS Transition
[*7] BSS Transition Management
[*8] http://w1.fi/hostapd/

表 3 実験で用いたソフトウェアのバージョンなど

ソフトウェア	バージョンなど
hostapd	v2.5（独自ビルド）
iOS[*10]	9.3.1
wpa_supplicant	v2.5（独自ビルド）

設定した．

実験では，実験システムを起動した直後にクライアント端末 1 台を AP_1 に接続し，hostapd のログ出力からクライアント端末の振る舞いを観察した．実験は，Apple iPhone 5c（iPhone と表記する），および Linux 向けの Wi-Fi クライアントツールである wpa_supplicant[*9]（Linux PC と表記する）の 2 台のクライアント端末について各々行った．

なお，hostapd 及び wpa_supplicant は，提案手法で求める BSS 移行管理を有効化するため，独自にオプションを付加してコンパイルしたものを使用した．また hostapd には，独自にバグ修正のためのパッチを当てている．

また，実験システムに用いた無線 LAN アダプタは

- WLI-UC-GNME（Buffalo 製）
- WLI-UC-GNM2（Buffalo 製)

であり，クライアント端末の一つに使用したアダプタは WN-G300UA（IO-DATA 製）あった．

4.1.1.2 結果

実験結果は次の通りである．

iPhone を実験システムの AP_1 に接続させたとき，AP_1 は 2 度 BSS 移行管理リクエストを送信したが iPhone からの返答はなかった．iPhone は 2 度目のリクエストの直後に AP_2 への移行し，実験システムは AP_1 の運用を中断した．なお，AP 間の移行には高速 BSS 移行が用いられた．

Linux PC は，1 度目のリクエストに対してステータスコードが 7（適した移行先候補がない）で返答した．その後，Linux PC は AP_1 との接続を続け，2 度目のリクエストに対してステータスコードは 0（受諾）で返答した．2 度目のリクエストの後，AP_2 へ（高速 BSS 移行ではなく）通常の再接続にて移行した．

4.1.1.3 考察

両クライアント端末の振る舞いは大きく異なっているが，これらに対しては BSS 移行管理によって AP を移行させることができた．

1 度目のリクエストに対する両クライアント端末の振る舞いは，各々がその時点で AP_2 の存在を確認できていないという理由で説明をつけることができる．実験システムの仕様では，AP_2 を立ち上げて直ちに BSS 移行管理リクエストを送信していたため，クライアントは AP_2 のビーコンなどを観測していなかったと考えられる．

4.1.2 高速 BSS 移行に特有の問題

高速 BSS 移行には，SSID を共有する AP 群の中でも特定のサブセット（モビリティ・ドメイン）の AP にだけ移行できるよう制限する仕組みが設けられている．高速 BSS 移行が行えるよう設定された各 AP は，MDID[*11] という 2 バイトの識別子を外部に公開することが求められている．すなわち，高速 BSS 移行を行うにあたっては，移行前と移行先の AP の MDID が一致している必要がある．また，高速 BSS 移行では，暗号化鍵の管理メカニズムが従来のものと異なっている理由から，モビリティ・ドメイン内で共通の R0KH-ID[*12] という識別子を外部に公開することも AP に求めている．これらの識別子も無論のこと，モバイルルータの位置トレースに利用される可能性がある．しかし，これらの識別子も 4.3 節で述べるものと同様に，識別子を共通化することで対策が可能である．

表 4 実験結果

	実験システムに接続した際の動作
iPhone	BSS 移行管理で応答はなく，2 度目のリクエストの直後に AP_2 への移行が行われた．移行には高速 BSS 移行が用いられた．
Linux PC	BSS 移行管理では 1 度目のリクエストに対してステータスコードが 7（適した移行先候補がない）の応答，2 度目のリクエストに対してステータスコードが 0（受諾）の応答が行われた．2 度目の応答の後，AP_2 へ（高速 BSS 移行ではなく）通常の再接続が行われた．

4.2 クライアント端末の MAC アドレス定期変更

前節の手法は BSSID のみを変更するもので，クライアント端末の MAC アドレスは変更しない．

クライアント端末は，通信を維持するためにそれ自体の MAC アドレスを維持するが，ユーザエクスペリエンスに支障のない範囲で接続を切断し，MAC アドレスを変更して再接続できる場面は存在しうる．クライアント端末はルータと異なり，ユーザと直接対話できるため，ユーザの様子を感知する，ユーザに接続を切断して良いか尋ねるといったことが可能である．このため，クライアント端末は AP との接続を切ってもユーザエクスペリエンスに影響がないかどうかを判断する能力があると考えられる．

Wi-Fi のクライアント端末はたいていの場合モバイル端末であるが，近年のモバイル端末向けのアプリケーションプラットフォームは以前と比べて，セキュリティや電力効率の観点からより制限の強い API を提供している．このほか，モバイル環境ではインターネットへの接続が喪失する機会の多いため，モバイル向けアプリケーションはそういった場合を想定して作られると仮定できる．

[*9] http://w1.fi/wpa_supplicant/
[*10] Cisco（http://www.cisco.com/）の登録商標である．
[*11] mobility domain identifier
[*12] pairwise master key R0 key holder identifier

4.3 DS 内の端末の MAC アドレスを共通化する

2.2.1 節で説明した通り，DS 内の端末の MAC アドレスも外部から観測可能である．前述した AP の移行においては，移行前後の AP の DS が共通であり，DS 内の端末のアドレスは変更されない．これは AP の移行前後で上位レイヤーのプロトコルの接続が維持されることの根拠であり，単純には DS 内の端末のアドレスを変更できない．そこで，本手法では DS 内の端末の MAC アドレスとしてモバイルルータ間で共通なものを利用することによってそれらの MAC アドレスを用いて端末の位置トレースを不可能にする．極端な例を示すと，全世界のモバイルルータが同じアドレスを DS 内の端末に割り当てていれば，攻撃者は DS 内のアドレスからモバイルルータを区別することができなくなる．

これによって，違いに無関係な異なる端末から同じ MAC アドレスを Destination などとして記したフレームが無線媒体にブロードキャストされることになるが，通信上の問題は発生しないと考えられる．これは，2.2.1 節で行った説明から，Receiver のアドレスが自身のものでない限り，DS 内デバイスの MAC アドレスを無線媒体上のデバイスは解釈しないと考えられるためである．

5. 制限

本論で提案した手法は，現行の 802.11 規格に基づいて市販されているクライアント端末に対しても有効であるが，現在市販されているものの内で対応できるクライアント端末は少ない．これは，802.11 規格に示されているが必須とされていない機能の実装を提案手法が求めているためである．提案手法ではクライアント端末には BSS 移行管理 (IEEE 802.11v) の実装を求めている．これに対応している端末に対して，Wi-Fi Alliance は Voice-Enterprise という認定プログラムを付与しており，この認定を受けている端末は 233 機種（2015 年 4 月現在）である．家庭向けの Wi-Fi 認証プロトコルを実装していることを示す WPA2[*13] - Personal の認定が 25374 機種（同）に付与されていることを踏まえると，Voice-Enterprise に認定されている端末は少ないことがわかる．

また，提案した手法はモバイルルータにおける位置プライバシ問題を解決するためのものであるが，対策は MAC アドレスに対するものに留まっており，SSID の問題に対しては別の対策を適用する必要がある．

6. 結論

本論では，Wi-Fi のモバイルルータにおける位置プライバシの問題をまとめ，そのうち MAC アドレスにまつわる問題に対して対策を提案した．行われた議論によると，提案手法は 802.11 規格を変更することなく実装可能であるが，一般に普及していない機能を要求しており，対策の普及には課題があることがわかった．

また，SSID にまつわる問題について，まだ本研究で求める制約にかなう手法が未発見である．このことから SSID にまつわる問題の解決が今後の課題であるといえる．

[*13] Wi-Fi Alliance の商標登録である．

参考文献

[1] IEEE: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* (2012).
[2] Whitley, E. A.: Informational privacy, consent and the “control” of personal data, *Information security technical report*, Vol. 14, No. 3, pp. 154–159 (2009).
[3] 高木浩光：高木浩光@自宅の日記 - Wi-Fi の MAC アドレスはもはや住所と考えるしかない，`http://takagi-hiromitsu.jp/diary/20111126.html`. Access date: 2016-04-19.
[4] Gruteser, M. and Grunwald, D.: Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis, *Mobile Networks and Applications*, Vol. 10, No. 3, pp. 315–325 (2005).
[5] Lei, M., Hong, X. and Vrbsky, S. V.: Protecting Location Privacy with Dynamic Mac Address Exchanging in Wireless Networks, *IEEE GLOBECOM 2007 - IEEE Global Telecommunications Conference*, pp. 49–53 (online), DOI: 10.1109/GLOCOM.2007.17 (2007).
[6] Greenstein, B., McCoy, D., Pang, J., Kohno, T., Seshan, S. and Wetherall, D.: Improving wireless privacy with an identifier-free link layer protocol, *Proceedings of the 6th international conference on Mobile systems, applications, and services*, ACM, pp. 40–53 (2008).
[7] Bernardos, C. J., Ziga, J. C. and O’Hanlon, P.: Wi-Fi internet connectivity and privacy: Hiding your tracks on the wireless Internet, *Standards for Communications and Networking (CSCN), 2015 IEEE Conference on*, pp. 193–198 (online), DOI: 10.1109/CSCN.2015.7390443 (2015).
[8] Huang, L., Matsuura, K., Yamane, H. and Sezaki, K.: Enhancing wireless location privacy using silent period, *Wireless Communications and Networking Conference, 2005 IEEE*, Vol. 2, IEEE, pp. 1187–1192 (2005).
[9] Jiang, T., Wang, H. J. and Hu, Y.-C.: Preserving location privacy in wireless LANs, *Proceedings of the 5th international conference on Mobile systems, applications and services*, ACM, pp. 246–257 (2007).
[10] Lindqvist, J., Aura, T., Danezis, G., Koponen, T., Myllyniemi, A., Mäki, J. and Roe, M.: Privacy-preserving 802.11 access-point discovery, *Proceedings of the second ACM conference on Wireless network security*, ACM, pp. 123–130 (2009).