交通流動センシングのための Wi-Fi パケットセンサの開発と性能実験

上善 恒雄[1]・三神山 駿[2]・辻本 悠佑[3]・望月 祐洋[4]・西尾 信彦[5]・西田 純二[6]

[1]非会員 工博 大阪電気通信大学教授 総合情報学部 (〒 575-0063 大阪府四条畷市清滝 1130-70)
E-mail: jozen@oecu.jp
[2]非会員 プロアクシアコンサルティング株式会社 (〒 530-0051 大阪市北区太融寺町 5-15)
[3]非会員 大阪電気通信大学大学院総合情報学研究科 (〒 575-0063 大阪府四条畷市清滝 1130-70)
E-mail: mw14a006@oecu.jp
[4]非会員 工博 立命館大学総合科学技術研究機構 (〒 525-8577 滋賀県草津市野路東 1-1-1)
E-mail: moma@ubi.cs.ritsumei.ac.jp
[5]非会員 立命館大学教授 理工学部 (〒 525-8577 滋賀県草津市野路東 1-1-1)
E-mail: nishio@cs.ritsumei.ac.jp
[6]正会員 株式会社社会システム総合研究所 (〒 550-0002 大阪市西区江戸堀 1-10-27)
E-mail: nishida@jriss.jp

概要: Wi-Fi を備えた電子機器から常時発信している電波に含まれる管理パケットデータには，その機器特有の識別子が含まれている．この識別子は二次的な個人情報として考えられる側面もあり，その扱いがビッグデータとしての社会的応用の可能性とプライバシー問題との狭間で議論が起きている．メールアドレスなど他の個人識別子と同様に，その活用と保護の使い分けとバランスが重要で，その妥協点を探る事が現時点で重要な研究課題である．将来的には通信をめぐる様々な規格は進化し変化していく事は間違いないが，通信を行う限り相手先を特定する何らかの仕組みは普遍的に残るはずであるし，むしろ積極的に Wi-Fi 等の無線技術を用いたプローブを作るという考え方は，場所の方にセンサを設置するため，GPS 電波の到達性に関係なく，地下街や建物内の特定エリアについても識別できる粒度の調整も可能になる．我々の研究グループで行っている Wi-Fi の管理パケットの観測にもとづく交通流動センサのこれまでの実験について報告するとともに，無線通信インフラを応用した交通流観測の可能性について整理する．

Key Words: *Wi-Fi, 流動センシング, プライバシー, ビッグデータ*

1. はじめに

Wi-Fi を搭載したスマートフォン等の情報機器の普及率が急伸しているが，これらの多くはスタンバイ状態であってもアクセスポイントとの接続を行うための Probe Request という管理パケットを送出している．Probe Request は常時 30 秒から 120 秒程度の間隔で発信されるようになっており，このパケットの中には発信した機器を特定する MAC アドレスが含まれているため，これをキーとして収集・分析すれば，情報機器利用者の流動・分布の状況を知る事が出来る．実際には情報機器利用者のプライバシに配慮して，取得した MAC アドレスを即座に，一意性は保ちながら利用者のアドレスがわからないような値に変換する必要がある．この変換は一方向性ハッシュ関数という写像を用いる．元の MAC アドレスの値は理論的には誰にも解読不可能ではあるが，異なった値は必ず異なった値に写像される関数である．これは異なる情報端末利用者の違いは識別しながら，その個人を特定出来ないようにする仕組みである．ただ，時間的・空間的に多くの情報から条件を絞り込んで行くと，その条件にあう少数の対象を推定できるようになるため，より厳格な対応を必要とされる場合は，後述するように応用可能性を犠牲にして時間的・空間的な制約をつける方法もとらなければならない場合もある．

本稿ではこのような一方向ハッシュ関数等による隠蔽のための変換後の MAC アドレスを匿名 (Anonymous)MAC アドレスとして，AMAC アドレスと略称する．また，このような Wi-Fi パケットセンサを”AMAC アドレス Probe センサ (略して AMP センサ)”と呼ぶ．この AMP センサの利用法としては，まずは AMP センサの周辺にある Wi-Fi 機器の数から，その付近での人の相対的な滞在数を推察する事が出来る．複数箇所に設置した AMP センサで収集した AMAC アドレスを分析すれば，ある匿名の個体の地点間の交通流動パターンの把握や移動速度を計測する事が出来る．スマートフォンを持つ歩行者の移動だけではなく，公共交通や自動車による移動の把握も可能である[1]．

[1] 高速道路における応用面について別途詳述する．西田他,”Wi-Fi パケットセンサーによる交通流動解析”, 本研究会に投稿予定.

本方式の人流把握手法はインフラコストが小さいため，人流密度の高い都市部だけでなく，スマートフォンが普及している地域であれば郊外や広く発展途上国への応用も期待できる．

さらに，プライバシ保護とは逆に，子供達の見守り等，積極的に所在地を知りたい場合は，AMAC アドレスに個人識別情報の識別子を付与して登録しておくことで，災害等の緊急時には収集された AMAC アドレスから対象となる個体の移動状況をリアルタイムに把握する事にも応用可能である． 本稿では第 2 章で今回構成した AMP センサの具体的なハードウェアとソフトウェアについて説明し，第 3 章でその AMP センサを用いた特性実験の結果について報告する．さらに第 4 章で AMP センサを使った簡易な人流センシング実験について報告し，第 5 章でプライバシ保護機能の強化について考察する．

2. システムの概要

(1) AMP センサのソフトウェア

Probe Request はオープンソースの Wireshark や TCPDUMP 等のスニフィングツールで取得できる．我々は低価格化，省電力化の目的で，ネットワークパケット捕捉のための pcap(packet capture) API のインプリメントである libpcap[3] を用いて Probe Request を取得し，即座に匿名化を行うモジュールと，得られた AMAC をインターネット上のストレージサーバにアップロードするモジュールを C 言語で，さらに NTP プロトコルによる精確な時刻合わせや、これらのモジュールの制御を行うスクリプトによってソフトウェアを構成している．

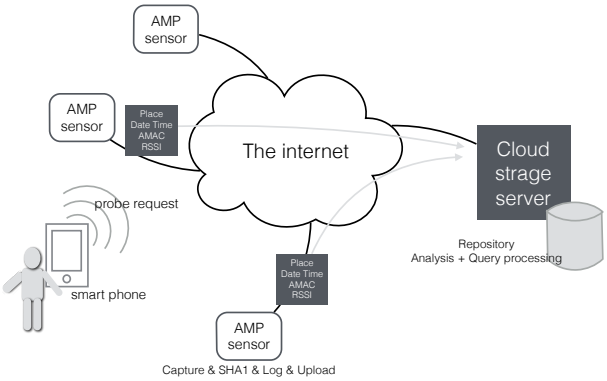
libpcap ライブラリにはフィルタ式として”type mgt subtype probe-req”を指定すると，管理パケットである Probe Request を受信したタイミングで準備したコールバック関数が呼び出される．

m_i を Probe Request から抽出した i 番目の MAC アドレスとし，その受信電波強度を $rssi_i$ とし，それを取得したタイムスタンプ（時刻＋日付）を t_i，場所を p_i とし，ここでは p_i は AMP センサを管理する識別子（番号）とし，実際の地理的な場所は別に管理する．また、関数 $anon(x)$ を一方向ハッシュ関数（今回の実験では SHA1(160bit)）等の匿名化関数と定義する．これらの値による組

$$R_i =< anon(m_i, t_i, p_i), t_i, p_i, rssi_i >$$

を基礎情報の単位として，ストレージサーバに格納する仕組みをベースとしている．この基礎情報から目的に応じた分析手法により可視化を行う．今のところ Web ベース (PHP と Javascript) アプリケーションと 3D ゲームエンジンを使ったエンタテイメント的な演出をしたアプリケーションを開発している．

今回の実験システムの全体概要を**図–1** に示す．



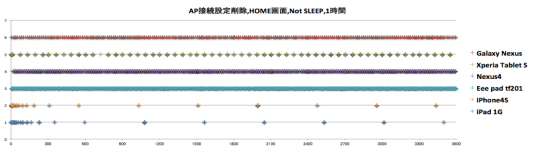
図–1 システム構成

(2) AMP センサのハードウェア

AMP センサのハードウェアとしては，monitor モードで動作する Wi-Fi アダプタと PC があれば良い．我々は安価なマイクロ PC(Raspberry PI) 上で Linux ベースで，Probe Request 取得専用の軽量プログラムを開発し，Kernel が起動後，NTP による時刻同期を確認してから Probe Request 取得プログラムを起動させるようにした．

(3) プライバシ保護

Wi-Fi 端末側には何も手を加えずに，Probe Request パケットをインフラ側で観測する事で人の交通行動（トリップ）をサーベイしようという今回の目的では，インフラ側に配置された AMP センサからの情報を統合するために，どうしてもキーとなる識別値が必要になる．その識別子として Wi-Fi 機器の MAC アドレスを元にするのだが，MAC アドレスは世界で一意性のある値であるため個人を識別できる個人情報，もしくは二次的な個人情報として扱われるため，何らかの変換が必要になる．その最低限の方法が一方向ハッシュ関数ではあるが，元の値 $m_i = m_j$ の時，それらのハッシュ値についても同じハッシュ関数 $hash()$ で写像したところで，$hash(m_i) = hash(m_j)$ が成立し，追跡は可能になり，それだけではプライバシ保護のためには不十分といえる．なるべく個人を識別する情報を取り扱わないでおこうとすると，できるだけ早い段階で統計値としてまとめてしまうことである．しかし，個人レベルのパーソントリップ調査で，細かな人流解析を行おうとすると，無闇に統計化するののではこの手法を適用する意味が無くなる．このあたりのトレードオフをどう考えるかは匿名化関数の構成法や，システムの運用



図–2 携帯端末からの Probe Request 送出頻度

方法によって段階的に調整可能である．

(4) ストレージサーバ

図–1 に示したように，AMP センサから送出される大量のデータを蓄積し，分析するためのクラウドストレージサーバシステムがもう一つの開発要素である．現時点では試験的な数個の AMP センサのみを対象としているため，実験施設に付帯している Wi-Fi 環境や LTE 等の無線ルータを介してインターネット接続し，レンタルサーバ上で MySQL に HTTP 経由で情報を集約し，計算処理を行っている．

今後，大量の AMP センサからの情報を処理するための開発目標として，分散型データベース処理エンジンを用いたクラウドサーバの構築を計画しており，すでに我々の研究チームでオープンソースの仮想クラウドサーバ 構築環境である CloudStack を活用したセンサデータ格納用ストレージサーバシステムのテストベッドを稼働している．また，HBase をベースとする時系列データベースである OpenTSDB，KairosDB などの動作検証とスキーマの検討を進めており，すでに HBase をベースとするスケーラブルなストレージシステムは構築を終えているので，データ量の増加に応じてスケールアウト可能で，高速データ処理を行う準備は整いつつある．

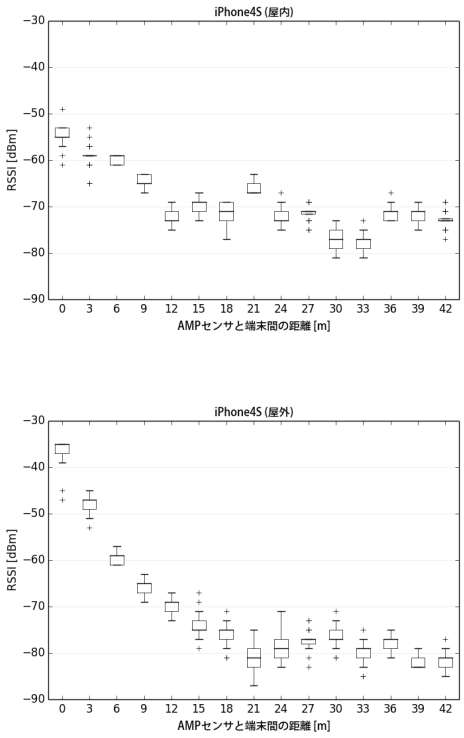
3. センサの基本特性

AMP センサの基本特性を知るために以下の基礎実験を行った．その結果について概要を述べる．

- 携帯端末からの Probe Request 送出頻度 (**図–2**)
- 屋内外での端末-センサ間距離による RSSI 特性 (**図–3**)
- 端末の装着・保持方法，障害物による RSSI への影響 (**図–4**)

これ以外に，これまで何度か Wi-Fi の電波特性について計測しており，すでに他学会等で報告 [1)2)] している．結論としては，以下のようにまとめることができる．

- RSSI はセンサ近傍数メートルだけ顕著に値が大きい．
- 数メートル以上は慣れると RSSI は 300 m まで増減するため、単純な反比例関係等は観測されない．



図–3 Probe Request の RSSI 距離減衰

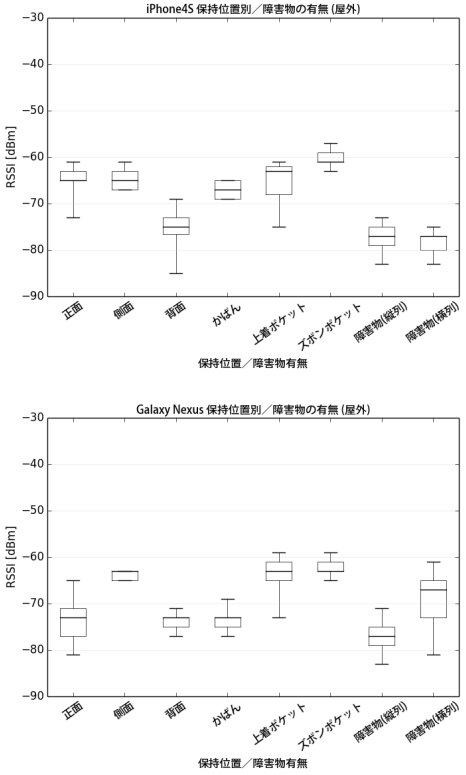
- センサと観測対象の Wi-Fi 機器の間に人が立つと急激に RSSI が減衰する．
- Wi-Fi 機器の持ち方によって RSSI が大きく変動する．

以上の事から，単純な RSSI の減衰量による内分や三角測量で距離を決定することは事実上不可能であるということがわかる．環境に設置するセンサやアクセスポイントの機器 ID をデータベースに登録する用法や，と端末側に距離測定用の特殊なプロトコルを実装する事で，精度の高い測量を可能にしている研究例はあるが，これらは測定対象者が積極的に端末側の仕組みをインストールして，起動しておく必要がある．

(1) 解析アルゴリズム

取得した Probe Request から得られるデータ R_i の集合からの解析手法について述べる．**図–2** に示した通り，Probe Request はアクセスポイントに接続していない場合，つまり携帯端末がアクセスポイントをアクティブに検索している場合で 15 秒から 120 秒の間隔で 1 度送出される．本報告では詳述していないが，携帯端末がフリー Wi-Fi アクセススポット等に接続した場合は時間オーダの非常に大きい値になる事もあるため，データ解析には若干の注意が必要である．

s 秒間隔で一度 Probe Request を送出する Wi-Fi 携



図–4 携帯端末の保持位置および障害物の有無の影響

帯端末を保持した人の，その地点での滞在時間を推定する場合を考える．特定のある AMAC アドレスを検知してから連続的にその場に滞在した後，その場を離れるという単純な場合で，Probe Request 取得を失敗しないという仮定をしたとしても $2s$ 秒の誤差があり得る．

s が大きい時，実際には滞在していなかったにもかかわらず，センサ捕捉範囲内に滞在していたという誤った結果が得られる場合もあり得る．この問題の対策について簡易的に処理するには Probe Request 取得の時間差にしきい値を設けるのだが，計測目的や対象場所によって調整するべき値になる．センサでのパケット収集は汎用の基礎情報としてデータを蓄積しておいて，この調整は解析時に行う事になる．

できるだけ精確に処理する場合は Probe Request 以外の管理パケットや，データパケットも取得すれば良いのだが，汎用の基礎情報としてデータを蓄積し，統計的知見を得るという基本的な目的を考えると，取得データが大きくなりすぎるし，プライバシ保護の観点からも問題を複雑にしてしまう欠点がある．

移動についての分析も同様ではあるが，センサを出来るだけ密に配置する事で，計測環境での電波強度分布の特性から確率モデルを構築し，精度の高い計測も可能になる．

これは本研究のようなインフラ側測位 [4] でも，Wi-Fi 環境の状況から端末側で測位計算を行う場合 [5] で同様の事が言える．

また，**図–3** では 40m 程度までの計測結果しか図示していないが，別の実験において，この 40m を超えた所から漸近的に推移し，使用機種にもよるが，300m 程度まで Wi-Fi 電波を観測する事ができる．そのため，もともと複数のセンサで同じ電波源である携帯端末を捕捉する事は珍しくなく，その計測粒度を細かくするには別の計算手法が必要になる．

Friis の伝達公式

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2$$

P_r : 受信電力
P_t : 送信電力
G_t, G_r : アンテナの利得

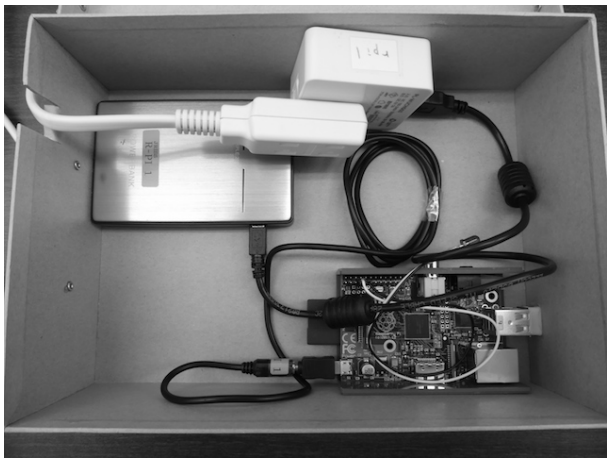
からも，電磁波の伝播損失は距離の 2 乗に反比例するという常識がある．それゆえ，単純な内分による位置推定の可能性を期待していた．

最近のスマートフォンでは IEEE802.11n 規格を搭載しているものもあり，ダイバシティアンテナ等による制御で，単純な電磁波源とは考えられなくなってきている．この問題に対処するために，[4] では隠れマルコフモデルによるビタビアルゴリズムを適用している．また，パケットの送出パターンや遅延等の固有特性から fingerprint（指紋）のような無線信号の固有パターンからデバイスを特定する研究もある [8]．

プライバシ対策も含めたインフラ側の測位方法として，Wi-Fi を計測するために同帯域の電波を使う ZigBee を利用して Probe Request の存在だけを検知し，密度の高い電波強度の測定を行うという，珍しい手法も提案されている [6]．

測位のためには直接役立たないかもしれないが，どういう携帯端末かを推測するために，Probe Request で送出されている SSID，すなわち日頃アクセスしている Wi-Fi アクセスポイントから他端末との関係性を推理するような手法は多くの研究例がある [7]．

良く知られている事だが，MAC アドレスの上位 24 ビットは OUI(Organizationally Unique Identifier)、最近は MA-L(MAC Address Block Large) と呼ばれ，これによりこのアドレスを使っている機器のメーカーが特定出来る．機種別に Probe Request の頻度や伝播特性にも個性があるので，メーカーと機種の情報もより精度の高い分析には役立てる事が出来る．



写真–1 設置用 AMP センサパッケージ

4. 実証実験

(1) 実証実験の概要

2014 年 1 月 29,30 日の二日間グランフロント大阪 the Lab の 2 階と 3 階に 6 台の AMP センサ (**図–1**) を設置して実証実験を行った．その後，2014 年 2 月 8,9 日でも大阪電気通信大学四條畷キャンパスにおいて，卒業研究発表展示会において AMP センサ 10 台を用いて本方式の実証実験を行った．

グランフロントの実験では，建物に大きな吹き抜け空間があり，複数の AMP センサで同時に同じ AMAC アドレスを多数観測した．鉄筋コンクリート造の異なる階であったため，RSSI からかろうじて分類が出来そうな値とはなったものの，the Lab は公開のオープンな環境でもあり，平面的な位置の特定は難しいという事を実感した．

大阪電気通信大学四條畷キャンパスでの実験では，4 つの建物に分かれて AMP センサを設置したため，建物間の移動状況を明確に把握する事が出来た．

(2) 告知

今回実験した 2 カ所は，the Lab ではグランフロント大阪の開業当初から，著者のグループも所属している VISLAB OSAKA という研究グループで，ビル管理者との合意の上で，別方式の人流解析実験を行っており，入り口に告知を行っているのと同時に，展示内容としてその解析結果を VISLAB OSAKA の展示ブースで常時展示している．そのため，今回はその実験の一環の追加実験として行った．しかし，プライバシ保護対策として，来街者に大しては，AMP センサ設置場所や入り口付近の数カ所に**図–5** の告知文を掲示した．

大学での実験はもともと卒業研究のための実験であり，やはり同様の説明文を AMP センサの設置場所と，

Wi-Fi パケット観測による流動調査を実施しています

■調査の目的と概要

- 立命館大学、大阪電気通信大学、帝塚山学院大学、㈱社会システム総合研究所では、総務省地域ICT振興型研究開発「うめきた」における Wi -Fi パケット・アノニマス人流解析システムの研究開発」の一環として、ナレッジキャピタル内で Wi-Fi パケットの観測実験を行っています。
- この調査は、皆様がお持ちのスマートフォン等が発する Wi-Fi パケットに含まれる情報を用いて、地区内の流動・滞留を把握し、防災計画・都市計画・商業活性化・交通計画など多方面で活用可能なアノニマス（匿名性）人流解析を行うことを目的に実施するものです。
- 調査期間 2014年1月29日（水）16:00 から 2014年1月31日（金）10:00 まで

■観測するデータとその取扱い

- みなさまがお持ちのスマートフォン等の Wi-Fi パケットに含まれる端末識別情報を端末が特定できない識別情報に変換（MAC アドレスを不可逆関数でハッシュ化）して記録します。通信内容を傍受するものではありません。
- この識別情報を含むパケットには、みなさまのお名前やメールアドレスなどの個人情報は一切含まれておらず、記録されたデータでは端末や個人を特定することはできません。
- 本調査の目的である流動・滞留解析以外には使用せず、また取得データを第三者に提供することはありません。
- 取得したデータは数学的・統計的に処理し、個人の行動追跡が行われることはありません。また複数日に渡る解析は行いません。

■観測を避けられたい場合は

- この調査では、お持ちのスマートフォン等の Wi-Fi パケットを自動的に観測しますが、もし **観測されることを望まれない方は、スマートフォンの Wi-Fi 機能をオフ** にしてください。この操作を行えば、お持ちの機器の Wi-Fi パケットが観測されることはありません。

■お問い合わせ先（お手持ちの機器のデータ消去を希望される場合など）

- この調査によりみなさまの個人情報や通信内容が取得されることはありませんが、もし観測されたデータの消去を希望される場合は、下記までお問い合わせください。お持ちの機器の MAC アドレスを教えていただければ、観測データの中から対応するデータをすべて消去いたします。

【実施者】 VisLab OSAKA 大阪電気通信大学総合情報学部 教授 上善恒雄
【連絡先】 ㈱社会システム総合研究所 大阪事務所 TEL 06－6441－1732
大阪市西区江戸堀1-10-27 （担当：大田、松葉、三神山）

図–5 Wi-Fi 計測の説明パネル

後述する展示ブースに取得したデータを使った応用アプリケーション説明員と共に告知をパネルを設置して周知に努めた．

(3) 可視化

最終的には統計値として公共の福祉に役立てるためとはいえ，使い方によっては施設側のメリットにはなっても観測対象者にはメリットとして感じられない場合もあり，プライバシ保護に関する配慮は欠かせない．

別の見方として，観測対象者という位置づけではなく，共に楽しむエンタテインメントとして，もしくは来場者にも明確なメリットがあるサービスとして実現する事がプライバシ対策として望ましい方向性の一つである．

大学での実験では，3 次元 CG のゲームエンジンをベースに，来場者を魔法使い等のキャラクタとして表現し，移動状況を可視化する応用アプリケーションを展示した (**図–2**).

この展示を見た来場者からはクレームは一つも無く，講義の出席システムや，ゲーム，見守りシステム等，様々な可能性について前向きなご意見を頂く事が出来た．結果としてこの展示会で優秀作品として保護者団体による展示全作品から選抜される後援会賞を受賞した．

写真–2 3D 可視化アプリケーション

5. プライバシ保護

(1) パーソナルデータのプライバシ保護の考え方

個人をある程度特定出来る可能性のある，本研究のような流れに対して，あらかじめ規制を設けるという発想もあり，プライバシ保護の観点から十分議論し，公共の福祉と個人の調停のバランスを決めるべきである．海外においても EU のデータ保護規則案 [9]，米国の消費者プライバシー権利章典 [10] など活発な議論が行われている．我が国の個人情報保護法における個人識別性について MAC アドレスが保護対象なるかどうかも議論のさなかであるため，我々としても，現時点では出来る限りの配慮をするしかない．現時点では我々のスタンスとしては個人情報保護法のコンセプトに従い，以下のポリシーで実験等を進めて行くことにしている．

- 計測するデータの利用目的の明示
- 計測するデータの内容とその取扱い方法の明示
- 計測されることを避けたい方への対策 (スマートフォンの Wi-Fi 機能をオフにする等) の明示
- 意思に反して自分のデータが取得された場合に, そのデータを消去するための申入れ先の明示と対策方法の準備 (オプトアウト対策)
- 計測データの分析のためのデータ保持期間を有期に設定し, 第三者提供を行わないことの明示

(2) 技術的対策

上記の倫理的な対応に加えて，技術的な対策も模索している．現時点では計測した MAC アドレスの秘匿は一方向ハッシュ関数のみに頼っているが，前述したように，ハッシュ化した値にも一意性があるため，MAC アドレスは秘匿したものの，厳密には端末の移動について追跡が出来る．勿論，もともとの目的のためには追跡可能でなければ意味が無い．本論のような ID 追跡によるトリップ推定手法は，個々の移動対象について出発地から到着地までの１トリップをデータとして得られる所に意味があり，平日・休日，季節，天候などによって人の移動特性がどう変わるかを詳細に検知出来ることが長所である．ある地点間の平均的トラフィックであればその経路上でのカウントでも数値を得る事が出来るため，本方式の，安価に人の流れを把握するメリットと，プライバシとは本質的に相反するものになっている．

そのため，MAC アドレスを直接使わず，Wi-Fi 電波に含まれる他の情報や伝播特性などで端末を特定するという方式 [5)~8)] を参考にしても問題のありかは変わらない．

今の時点でプライバシ保護のために計測データの処理に工夫をするとすれば，第 2 章で述べた匿名化関数 $anon(m_i, t_i, p_i)$ にタイムスタンプと場所のパラメータを入れているように，時と場所によってハッシュ値をそれらのパラメータによって変化させることで，時空間でデータの分離が可能になり，その限られた時空間のみでのデータ処理を行う事で，プライバシ保護の側に寄る事は出来る．その具体的な分割方法や運営方法には様々なバリエーションが考えられるが，その基本方針としては，実現可能性も含めて次に打てる手段であることは間違いない．

6. おわりに

本研究で扱っている Wi-Fi による個人識別は，あくまでも過渡期のものである．データリンクレイヤには本来，世界的な一意性のあるアドレスを用いる必要は無く，同じネットワークセグメント内だけで一意であればよいので，次世代のデータリンクプロトコルでは MAC アドレスによるプライバシ問題は解決していることに違いない．それと同時に本研究のような簡易で安価な交通・人流の測定方法も次の方法を開発する必要がある．

技術の変遷とともに問題も手法も変わって行くが，防災・安全・快適なまちづくりのための基礎情報は誰もが望むものであるはずであるし，これまでの諸問題を考慮した上で積極的に来街者がデータを発信するような仕組みは現在でも構築可能である．最も重要なのはこのような基礎情報の重要性を認識し，その整備に誰もが参加するという意識である．

謝辞: 本研究の一部は総務省の「戦略的情報通信研究開発推進制度 (SCOPE)」(受付番号 132307011) の支援を受けて実施された

参考文献

1) 望月祐洋, 上善恒雄, 西田純二, 中野秀男, 西尾信彦:”Wi-Fi パケットセンサを利用した匿名人流解析システムの構築”, 情報処理学会ユビキタスコンピューティングシステム研究会,IPSJ SIGUBI Technical Report, 2014.
2) 三神山駿, 森本哲郎, 白濱将太, 上善恒雄: ”ProbeRequet を利用した人流解析システム”, 第 12 回情報科学フォーラム（FIT2013）講演論文集,M-010,2013.
3) Carstens, T.: ”Programming with pcap”, http://www.tcpdump.org/pcap.html, Apr.2014 参照.
4) Musa, A.B.M.,Eriksson, J.: ”Tracking unmodified smartphones using wi-fi monitors”, SenSys ’12 Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems,2012.
5) Kessel,M., Werner,M.: ”SMARTPOS: Accurate and Precise Indoor Positioning on Mobile Phones”,Konferenzen und Journale, MOBILITY 2011 : The First International Conference on Mobile Services, Resources, and Users, 2011.
6) Lim,R.: ”Tracking smartphones using low-power sensor nodes”, SenSys ’13 Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems Article No. 52, ACM,2013.
7) Barbera, M.V., Epasto,A.,Mei,A., Perta,V.C.,Stefa,J.: ”Signals from the crowd: uncovering social relationships through smartphone probes”, IMC ’13: Proceedings of the 2013 conference on Internet measurement conference, October 2013.
8) Desmond,L.C.C., Yuan,C.C., Pheng,T.C.,Lee,R.S.: ”Identifying Unique Devices through Wireless Fingerprinting”, WiSec ’08 Proceedings of the first ACM conference on Wireless network security, Mar.2008.
9) European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) ,2012.
10) White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy,2012.

A performance experiment of the Wi-Fi packet sensor for traffic flow sensing

Tsuneo JOZEN, Shun MIKAMIYAMA, Yusuke TSUJIMOTO, Masahiro MOCHIZUKI, Nobuhiko NISHIO, Junji NISHIDA