無線LAN位置推定におけるプライバシ保護

彭 作涛[1,a)]　梶 克彦[1,b)]　河口 信夫[1,c)]

概要：近年，無線 LAN 位置推定サービスの利用が広がると共に，位置情報プライバシ侵害の問題が指摘されている．既存の無線 LAN 位置推定サービスでは，ユーザの移動履歴，位置情報などが不正に取得され，個人のプライバシが侵害される可能性がある．本研究では無線 LAN 位置推定におけるプライバシの問題を解決する手法として，空間的な確からしさと時間的な確からしさを考慮したユーザの信頼性判定アルゴリズムを提案する．さらに，我々は無線 LAN を用いた位置情報・測位に関するポータル Locky.jp を運営している．Locky.jp のデータベースに格納された基地局の観測データを対象とし，本手法を検証する．

Privacy Protection in Wireless LAN-based Location Estimation

Zuotao Peng[1,a)]　Katsuhiko Kaji[1,b)]　Nobuo Kawaguchi[1,c)]

1. はじめに

現在，無線 LAN 位置推定技術の発展により，様々な無線 LAN 位置推定システムや，それらを用いた位置情報サービスの提案が多く行われてきた [1], [2], [9], [10]．同時に，無線 LAN 機能を搭載したモバイル端末の普及，多くの人々が無線 LAN 位置推定サービスを利用できるようになりつつある．

無線 LAN を用いた位置推定システムは，事前に様々な地点で収集された基地局の位置情報や電波強度などの情報をもとに，ユーザが観測した基地局情報を用いて，ある手法で位置推定が行なわれる [13].

無線 LAN 位置推定サービスの普及に伴い，無線 LAN 位置推定システムにおけるプライバシ問題も意識されている．特に，近年 GPS と無線 LAN 機能を搭載したスマートフォンの普及により，GPS による位置と無線 LAN 基地局情報が世界的に集められてきている．これらの情報をインターネットに公開しているので，位置情報プライバシに関する懸念が生じる．Nils らは基地局の偽装などの手法を用いて，基地局所持者の位置情報が特定されることを示した [3]．つまり，悪意があるユーザは基地局の偽装によって基地局所持者の位置情報や移動履歴などを不正に把握している可能性がある．そのため，今後無線 LAN 位置推定サービスが普及するためには，ユーザのプライバシを保護しつつも，ユーザが有用なサービスを享受できる環境を実現する必要がある [11].

無線 LAN 位置推定におけるプライバシ侵害とは，悪意のあるユーザにより，他人の無線 LAN 基地局情報や受信履歴などを入手し，無線 LAN 位置推定サービスによって，他人の位置情報，移動履歴などを窃取する行為である．

他人の無線 LAN 基地局情報や受信履歴などを入手する手法として，基地局の情報を把握した上での販売，贈与が考えられる．その他にも，インターネット上で公開されている基地局の情報も悪用される可能性がある．

既存の無線 LAN 位置推定サービスでは，ある基地局の情報（BSSID，電波強度など）をサーバ側に問い合わせて，この基地局の位置情報を取得することが可能である．このため，攻撃者は前述の方法で，ユーザの無線 LAN 情報や受信履歴を入手していれば，位置情報サービスにその情報を送って，このユーザの位置や移動履歴を捕捉できてしまう．このようにユーザの位置情報，移動履歴などが不正に取得され，個人プライバシが侵害される可能性がある．例えば，図 1 のように, 事前に基地局 A の情報をサーバに送られ，データベースに格納されているとする．攻撃者は何らの方法で基地局 A の情報を知って，偽りの無線 LAN 環境を構築し，基地局 A の情報をサーバに送ることにより，

[1] 名古屋大学大学院工学研究科
Graduate School of Engineering,Nagoya University
[a)] peng@ucl.nuee.nagoya-u.ac.jp
[b)] kaji@nuee.nagoya-u.ac.jp
[c)] kawaguti@nagoya-u.jp

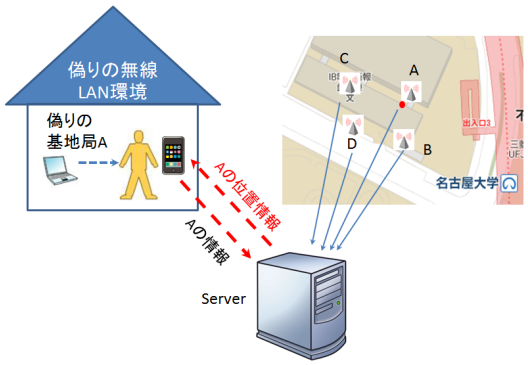

図 1 プライバシ侵害の例

基地局 A（基地局 A の所持者）の位置を捕捉できてしまう．これで，特定の基地局を追跡することが可能になり，個人の家の場所などが特定でき，ストーキング等の犯罪行為につながる恐れがある．

本研究では，以上で述べたような無線 LAN 位置推定におけるプライバシの問題を解決する手法として，空間的な確からしさと時間的な確からしさを考慮したユーザの信頼性判定アルゴリズムを提案する．また，無線 LAN プライバシ保護とユーザの利便性のトレードオフを把握するために，事前に様々な地点で無線 LAN 観測データを大量に収集した Locky.jp のデータベースを用いて，評価実験を行う [12].

本稿の構成は以下のとおりである．2 章において，Google 社の対策について述べ，3 章において基地局の電波受信確率モデルを構築する。4 章は空間的な確からしさと時間的な確からしさ両方を考慮し，ユーザの信頼性を判断する．次に 5 章では本手法の評価実験について述べ，最後に 6 章においてまとめと今後の課題を挙げる．

2. Google 社の対策

Google 社は，世界中の多くのユーザの協力のもとで，大量の無線 LAN データを収集し，Google Location Server に大規模データベースを構築している．これらに基づいて，GPS，IP アドレスと無線 LAN を併用し，位置情報サービスを提供している．

2011 年，米 CNET がプライバシに関する懸念を指摘する記事を掲載した後，同年 11 月にプライバシポリシーとして，Google 社は位置情報データベースから無線 LAN 基地局を除外するオプトアウト方法を発表した [8]．具体的には，Google に位置情報を利用されたくない場合，アクセスポイントの名称（SSID）の最後に「`_nomap`」を追加して，オプトアウトできる．たとえば「`Nuwnet`」という名称の無線 LAN 基地局であれば，「`Nuwnet_nomap`」に変更すると，この基地局の位置情報を Google のサービスから排除可能となる．

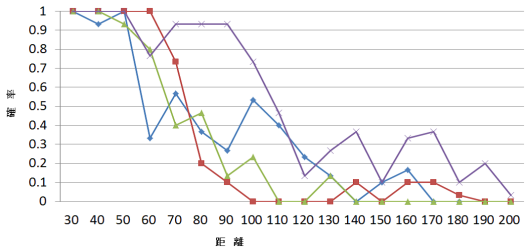

図 2 距離と無線 LAN 観測確率の関係 (基地局ごと)

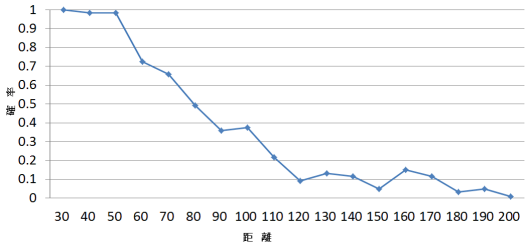

図 3 距離と無線 LAN 観測確率の関係 (全ての基地局の平均)

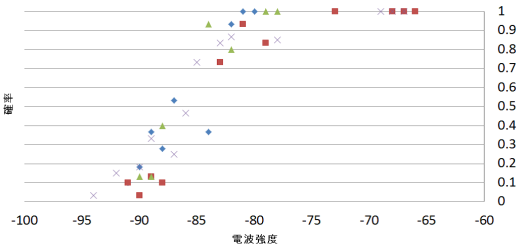

図 4 電波強度と無線 LAN 観測確率の関係 (基地局ごと)

3. 基地局の電波受信確率モデル

本研究では，ユーザ又は端末が推定位置で観測されるはずの基地局が求められるため，ある地点で各基地局の電波が受信される確率を求める必要がある．つまり，基地局の電波受信確率モデルを実験により構築する必要がある．

基地局の電波受信確率モデルとは，基地局からの距離と基地局の電波が受信される確率の関係である．このモデルを構築するために，我々は実験を行った．実験の場所は名古屋大学豊田講堂前である．実験の方法としては，先に 4 つの基地局を設定しておき，基地局からの距離が 30m から 200m まで 10m ごとに基地局情報を測定する．一つの観測点で 1 分間を立ち止まって，2 秒ごとに一回スキャンし，基地局の情報を測定する．つまり、各観測点で 30 回の測定結果を記録する．観測点ごとに，ある基地局が観測される回数を $count$ とし，この基地局の電波が受信される確率 P_{rev} を次の式で示す．

$$P_{rev} = count/30 \tag{1}$$

実験の結果については，図 2 と図 3 が距離と受信される確率の関係図（基地局の電波受信確率モデル）であり，図 4 と図 5 は電波強度と受信される確率の関係図である．

図 4 と図 5 によって，電波強度が大体-80dBm より強い

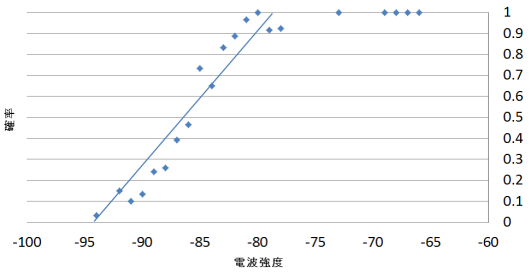

図 5 電波強度と無線 LAN 観測確率の関係 (全ての基地局の平均)

場合で基地局の電波が受信される確率が 1 であり，-80dBm から-95dBm まで，電波強度と受信される確率の関係は直線関係と見なされる．これにより，電波強度と受信される確率の関係が次の式で示される．確率的なモデルであるため，$PL \leq -95$ の時に，$P_{rev}(PL) = 0$ ではなく，非常に小さい値を入れるとよいと考える．

$$P_{rev}(PL) = \begin{cases} 1 & (PL \geq -80) \\ \frac{PL}{15} + \frac{19}{3} & (PL \in (-80\ , -95)) \\ 10^{-3} & (PL \leq -95) \end{cases} \quad (2)$$

なお，無線 LAN 基地局の電波伝搬モデルの基本的な式を次の式に示す [4].

$$PL = UL + 10n\log(d) \quad (3)$$

式 (3) において，d は基地局からの距離である．UL は参考距離 1m において観測できる受信電波強度であり，定数 n は物理環境の障害物等により設定するパラメータである．一般的には $UL = -32dBm$ と設定する [5], [6].

式 (2) と式 (3) を用いて，基地局からの距離と受信される確率の関係 (基地局の電波受信確率モデル) が次の式で示される．前述のように，$d \in (10^{\frac{63}{10n}}, 200)$ の時に，$P_{rev}(d) = 0$ ではなく，非常に小さい値を入れるとよいと考える．

$$P_{rev}(d) = \begin{cases} 1 & (d \leq 10^{\frac{24}{5n}}) \\ \frac{21}{5} - \frac{2}{3}n\log(d) & (d \in (10^{\frac{24}{5n}}\ , 10^{\frac{63}{10n}})) \\ 10^{-3} & (d \in [10^{\frac{63}{10n}}\ , 200]) \end{cases} \quad (4)$$

実験環境定数 $n = 2.88$ のときの式 (3) のモデルを図 6 に示した．この場合，基地局の電波受信確率モデルと実験データの比較を図 7 で示す．

以上より，本モデルが実験データに適合することが確かめられた．

4. ユーザの信頼性判断アルゴリズム

無線 LAN 位置推定におけるプライバシ問題の本質は，攻撃者が実際に基地局の近くに行かずに，基地局の位置情報を窃取できるところにある．そのため，無線 LAN プライバシ侵害を解決するポイントは，ユーザ (または位置推定端末) が推定位置にいるかどうかの信頼性を判断する方法と考えられる．

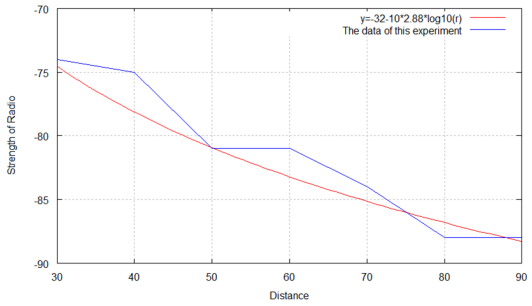

図 6 距離と電波強度の関係（n=2.88）

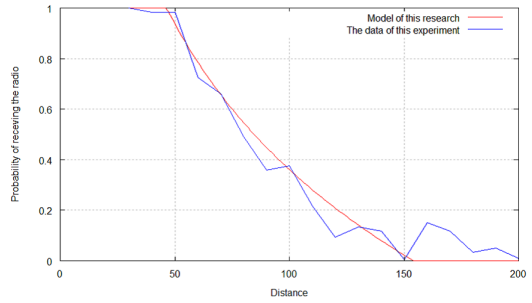

図 7 本モデルと実験データの比較

例えば，図 1 に示した例のように，基地局 A の情報のみをサービス提供側に送ったとする．ここで，基地局 A が存在するエリアには，基地局 B，基地局 C，基地局 D が共に存在する場合，基地局 B，C，D は基地局 A と共に観測できる可能性が高いと考えられる．特に基地局同士の実際の位置が極めて近い場合，どこから観測しても共に観測される可能性が極めて高い．その場合に，ユーザの送信情報の中にこれらの基地局同士が同時に送信されなかったら，ユーザが本当にその場にいるのか疑いが生じる．

さらに，観測される基地局が全て送信された場合でも信頼できない可能性がある．例えば，ユーザが十秒前にいた場所が分かったとする．ユーザの移動速度には限界があるため，十秒後に存在できる場所は限定され，移動距離は一定範囲内にとどまる．このように，時間によりユーザの大まかな移動距離を判断できる．もしユーザの推定移動距離が非現実的な場合，ユーザが本当にその場にいるのかが疑われる．

以上から，本研究での無線 LAN プライバシ侵害問題の解決手法は，ユーザがある時点，ある地点にいるとき，観測されているはずの空間的な情報，時間的な情報を用いて，その地点にいる確からしさを求めることである．

本稿で提案するアルゴリズムの流れを図 8 で示す．まず，ユーザが観測した基地局情報に基づいて，位置推定を行う．次に，推定位置で観測された基地局情報と基地局の電波受信確率モデルによって，空間的な確からしさを計算する．同時に，一定時間以内の履歴により，推定位置での時間的な確からしさを計算する．最後に，空間的な確からしさと時間的な確からしさ両方を考慮し，ユーザの信頼性

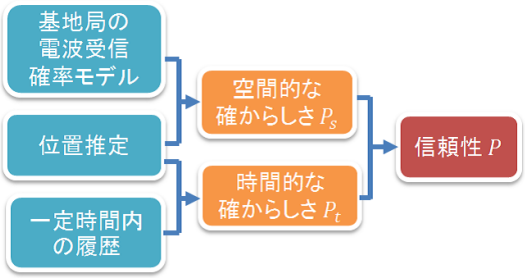

図 8 提案アルゴリズムの流れ

を判断する手法を考える．

4.1 空間的な確からしさ

空間的な確からしさとは，ある地点で観測された各基地局について，同時に観測されるはずの基地局と観測されないはずの基地局が観測されているかどうかにより，ユーザがその場所にいる可能性を表すものである．

4.1.1 前提

無線 LAN 位置推定サービスは無線 LAN データベースに依存する．しかし，新規基地局が設置される可能性があるため，データベースの中に存在しない基地局がユーザの信頼性に影響を与えないと考える．したがって，本研究で扱う基地局は無線 LAN データベースに格納された基地局のみとする．

4.1.2 計算方法

ユーザが受信した基地局情報集合を O とする．受信した基地局情報 o_n は，基地局の BSSID b_n と受信電波強度 r_n の組として保存される．

$$O = \{o_1, o_2, ..., o_n\} \tag{5}$$

$$o_n = (b_n, r_n) \tag{6}$$

まずは，式 (5)(6) の情報を用いて，ある位置推定手法でユーザの位置 $p(x, y)$ を推定する．

次に，ユーザの推定位置で以下の 1) と 2) の 2 種類の基地局が考えられる．これらに基づいて，図 9 で示した流れに従って，ユーザがこの点にいる空間的な確からしさ P_s を計算する．

1) 観測された基地局 (集合 A).

2) 観測されるはずだが，観測されなかった基地局（集合 D).

1) について，データベースに存在しない観測された基地局が推定位置で受信される確率を 1 とする．他の各基地局と推定位置の距離を算出し，式 (4) で示された基地局電波の受信確率モデルを用いて，これらの基地局が推定位置で受信される確率を計算する．以上により，観測された各基地局 b_n が推定位置 $p(x, y)$ で受信される確率 P_{okn} が求められ，集合 P_{ok} とする．

$$P_{ok} = \{P_{ok1}, P_{ok2}, ..., P_{okn}\} \tag{7}$$

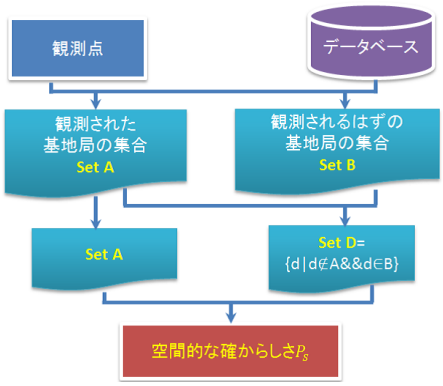

図 9 空間的な確からしさの計算

2) について，データベースにより推定位置から誤差を考慮した距離が 200m 以内の基地局を求め，観測されるはずの基地局とする．基地局の電波受信確率モデルにより，各基地局 d_m がユーザの推定位置 $p(x, y)$ で受信される確率 p_{ngm} の集合を P_{ng} とする．

$$P_{ng} = \{P_{ng1}, P_{ng2}, ..., P_{ngm}\} \tag{8}$$

以上から，1) と 2) の基地局がユーザの推定位置で観測される確率を用いて，ユーザはこの地点で基地局情報 O を取得する確率 $P(P_{ok}, P_{ng})$ が求められる．

$$P(P_{ok}, P_{ng}) = \prod_{i=1}^{n} P_{oki} \prod_{j=1}^{m} (1 - P_{ngj}) \tag{9}$$

表 1 最大確率を求める

Algorithm MaxProb _Calculating(x,y)

$P = 1$, $P_{all} = P_{ok} + P_{ng}$
for every item $P_i \in P_{all}$ do
  if $P_i \geq 0.5$ do
    $P = PP_i$
  else
    $P = P(1 - P_i)$
  endif
endfor
return P

関連基地局個数が $(m + n)$ である場合，ユーザの受信状況は 2^{m+n} パターンがある．これらのパターンの中で，最大確率を持つパターンの空間的な確からしさが最大だと考えられる．表 1 で示したアルゴリズムで最大確率を求めて，空間的な確からしさ P_s を次の式で定義する．

$$P_s = \frac{P(P_{ok}, P_{ng})}{\textbf{MaxProb\_Calculating(x,y)}} \tag{10}$$

4.2 時間的な確からしさ

時間的な確からしさは，ある程度の位置情報の履歴から推測される単位時間前の移動速度を用いて，移動速度の限界と平均加速度に基づいて，現在の無線 LAN 情報による推定位置の合理性を表すものである．

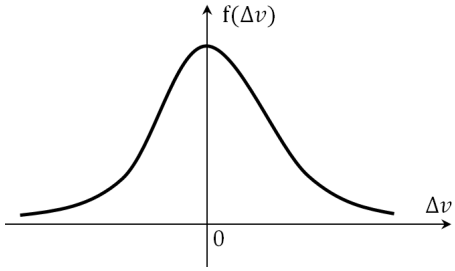

図 10　平均加速度

4.2.1　前提

時間的な確からしさは移動範囲の合理性を表すものであるため，ユーザ（端末）は移動するときに限り，時間的な確からしさが発生する．ユーザ（端末）が移動しないと，単位時間前の時間的な確からしさと同じにすると考える．

4.2.2　単位時間前の移動速度

一定時間内におけるユーザの移動速度は安定し，大きな変化がないと推定できるため，単位時間前の一定時間以内の移動速度が現在移動速度の合理性を評価するための 1 つの基準と考えられる．本研究は一定時間 T 内の N 回の履歴を利用し，単位時間前の移動速度 v を算出する．位置推定の時間間隔を $\triangle t$ とすると，履歴上の各時間間隔の平均速度が求められる．選定した履歴内，現時点と近い順で $\triangle t$ 時間ごとの速度を$\{v_1, v_2, ..., v_N\}$ とし，ユーザの単位時間前の移動速度 v を次の式で定義する．

$$v = r \cdot v_1 + \frac{r}{2} \cdot v_2 + ... + \frac{r}{2^{N-1}} \cdot v_N$$
$$(r = \frac{2^{N-1}}{2^N - 1}) \tag{11}$$

式中の $\frac{r}{2^{N-1}}$ は割引率である [7]．これにより，ユーザの最近の履歴を重視し，過去一定時間内の移動速度も適当に反映できる．

4.2.3　平均加速度

単位時間前の移動速度と現在の $\triangle t$ 時間内の推定平均速度の変化を平均加速度 $\triangle v$ と定義する．$\triangle v$ が 0 である場合，時間的な確からしさが一番大きいと考えられる．さらに，$\triangle v$ が大きくなると時間的な確からしさが下がると考える．$\triangle v$ は正規分布 $N(0, \sigma^2)$ に従うと考えられ，図 10 のように示される [15][16]．分散 σ^2 は移動手段により違う．

$$f(\triangle v) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp(-\frac{\triangle v^2}{2\sigma^2}) \tag{12}$$

4.2.4　計算方法

速度の限界と平均加速度両方を用いて，時間的な確からしさを算出するため，ユーザの移動速度の限界を V_{max} と設定する．

時間的な確からしさの計算は図 11 で示された流れで行われる．まず，単位時間前の移動速度 v を求めるため，最初に利用可能な移動履歴があるかどうか判断する．利用可能な履歴がない場合，時間的な確からしさ $P_t = 0$ とする．

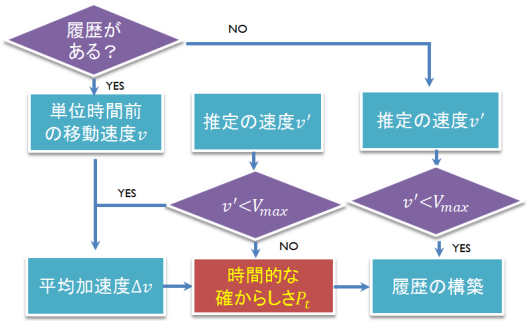

図 11　時間的な確からしさの計算

推定速度 v' が V_{max} より小さければ，履歴を構築する．利用可能な履歴があれば，4.2.2 節の手法で単位時間前の移動速度 v を計算する．

次は，現在の移動速度 v' と平均加速度 $\triangle v$ を計算する．位置推定の関数を $loc(t)$ とし，距離計算関数を $dis(p_1, p_2)$ とすると，ユーザの推定移動距離 d_w を式 (15) で示す．

$$d_w = dis(loc(t_i), loc(t_{i-1})) \tag{13}$$

これより，ユーザの現在の移動速度 v' と平均加速度 $\triangle v$ は次の式で示される．

$$v' = \frac{d_w}{\triangle t} \cdot r + \frac{v}{2} - \frac{v_N}{2^N} \cdot r \tag{14}$$

$$\triangle v = \frac{v' - v}{\triangle t} \tag{15}$$

以上により，時間的な確からしさ P_t を次の式で定義する．

$$P_t = u(V_{max} - v')\frac{f(\triangle v)}{f(0)} \tag{16}$$

$u(x)$ は単位階段関数である．$x \geq 0$ の時，$u(x) = 1$ であり，$x < 0$ の時，$u(x) = 0$ である．

4.3　ユーザ信頼性の判断

本研究では空間的な確からしさ P_s と時間的な確からしさ P_t 両方を考慮し，ユーザの信頼性を判断する．空間的な情報と時間的な情報の両方が満たされるときに限り，ユーザを信頼できるため，ユーザの信頼性 P を式 (19) とする．

$$P = P_s \cdot P_t \tag{17}$$

5.　評価実験

プライバシを守るため，一定の使用利便性を犠牲にする必要がある．無線 LAN 位置推定におけるプライバシ保護とユーザの便利性のトレードオフを把握するため，Locky.jp のデータベースに基づいて本評価実験を行う．

5.1　実験設定

5.1.1　パラメータの設定

本稿で言及した各パラメータの設定は表 2 に示す．本実

験は 300 秒以内の履歴のみを利用する．位置推定間隔は Locky.jp のデータ収集の間隔と同じように 2 秒と設定する．そして，一般的に自動車が最大加速度を持っているため，自動車の加速度モデルにより σ^2=2 と設定する [16]．速度の制限は新幹線の速度，100 m/s と設定する．最後にユーザを信頼できるかどうかの閾値を 0.5 とする．

表 2 パラメータの設定

パラメータ	T	$\triangle t$	σ^2	V_{max}	閾値
値	300 s	2 s	2	100 m/s	0.5

5.1.2 実験データの設定

本実験は Locky.jp のデータベースを 2 つの部分に分けて，それぞれ学習データと評価データとする．各部分の概要は表 3 と表 4 に示す．学習データに基づいて，評価データを評価するため，学習データを完全に信頼する必要がある．

表 3 学習データ

観測情報の数	基地局の数	観測期間
10471524	756415	2005/7/6 - 2010/3/3

表 4 評価データ

観測情報の数	観測点の数	観測期間
6958	2917	2010/3/3 - 2010/4/9

5.1.3 位置推定

位置を推定できる場合のみプライバシ保護問題があるため，本稿におけるプライバシ保護問題の検証のため，事前に位置推定が必要である．ここでは proximity 手法で各観測点の位置を推定する [13]．結果として 2917 個の観測点の中で，1259 個の観測点の位置を推定できた．そのため，本評価実験は位置を推定できる 1259 個の観測点を対象として行う．

5.2 実験の結果

5.2.1 計算結果

本稿の手法により，評価データの各観測点の空間的な確からしさ，時間的な確からしさ，信頼性それぞれを計算した．結果は図 12，図 13，図 14 に示す．

5.2.2 計算時間

本実験の動作環境については，CPU が 2.8GHz であり，メモリが 16G である．計算時間は表 5 に示す． 1 つの観測点において，空間的な確からしさの計算は約 1 秒がかかり，位置推定と時間的な確からしさの計算にかかる時間はそれぞれ 0.0014 秒と 0.0008 秒以下がかかる．実際に，位置推定と空間的な確からしさの計算はデータベースと問い合わせる必要があるため，計算時間がデータベースの大きさに依存する．

表 5 計算時間

	観測点の数	かかる時間 (s)	平均時間 (s)
位置推定	2917	4	0.0014
空間的な確からしさ	1259	1304	1.0357
時間的な確からしさ	1259	1 以下	0.0008 以下

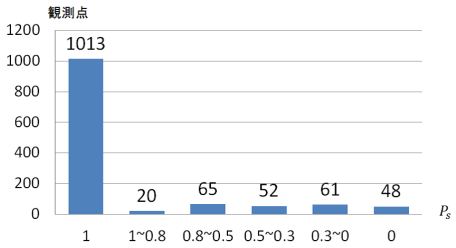

図 12 空間的な確からしさの計算結果

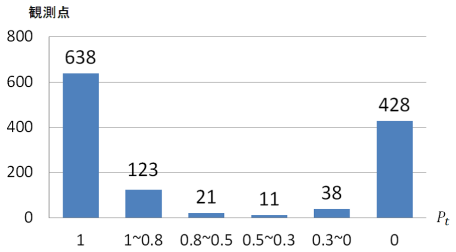

図 13 時間的な確からしさの計算結果

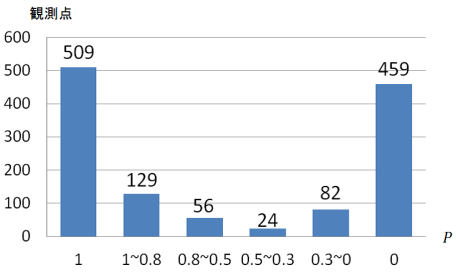

図 14 信頼性の計算結果

5.2.3 信頼率

表 2 の閾値により，評価データ全体の各観測点の空間的な確からしさ，時間的な確からしさ，信頼性それぞれに基づく信頼率を計算する．結果は表 6 に示す．

結果により，信頼性で判断する信頼率は約 55%に留まった．実際のデータを見ると，ユーザが 1 つの地点で何秒間か立ち止まった場合がある．信頼性が低い地点で立ち止まっても信頼性が 0 のままである．たとえば，最初の 67 個の観測点 (134 秒) の推定位置はすべて共通である．これらは履歴がないため，信頼性は全て 0 になった．

表 6 信頼率

	空間的な確からしさ	時間的な確からしさ	信頼性
信頼率	87.21%	62.11%	55.12%

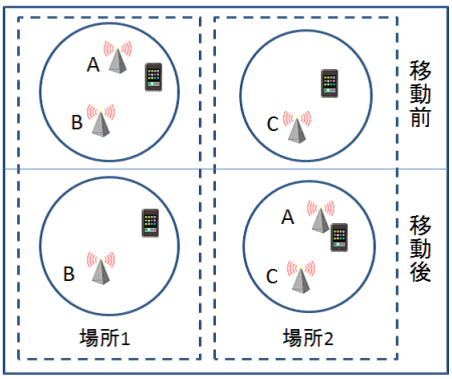

図 15　プライバシ侵害データ

5.3　検証実験

5.3.1　プライバシ侵害データの抽出

移動した基地局は無線 LAN 位置推定精度に悪影響を及ぼす．本実験の学習データでは，移動した基地局データは削除した [14]．しかし，評価データの中には，移動した基地局データも含まれている．

悪意があるユーザは他の場所にある基地局の情報を入手し，位置推定サービスにより，その基地局の位置を獲得して，基地局所持者のプライバシを侵害する．以上の状況を評価データの中の移動した基地局データを用いてシミュレーションしたい．そこで，本稿では移動基地局を含む観測データを利用する．

たとえば，図 15 に示すように，移動前，基地局 A，B が場所 1 にあり，基地局 C は場所 2 にあるとする．場所 1 にある端末の proximity 手法による推定位置が基地局 A の位置であり，場所 2 にある端末の推定位置は基地局 C の位置である．移動後，場所 1 にある端末の推定位置が基地局 B の位置となり，場所 2 にある端末の推定位置が基地局 A の位置となる．学習データ (移動前) を完全に信頼すると，評価データ (移動後) では場所 2 にある端末の推定位置が場所 1 になった．

プライバシ侵害のシチュエーションとして，場所 2 にいる攻撃者は何らかの方法で基地局 A の情報 (BSSID など) を知っていれば，場所 2 で偽りの基地局 A の環境を構築して，無線 LAN 位置推定システムにより基地局 A の位置を獲得する，学習データ (移動前) により，基地局 A の位置は場所 1 である．つまり，攻撃者は場所 2 にいるが，基地局 A の情報を利用して，基地局 A（場所 1）の位置を獲得し，基地局 A の所持者のプライバシを侵害した．

以上から，移動した基地局を含む観測点はプライバシ侵害と同じシチュエーションを示していると言える．

本実験の評価データの中に，移動距離が 200m 以上の基地局データを含む観測点は 87 個がある．これらの観測点をプランバシ侵害データとして，本研究のプライバシ保護手法を検証する．

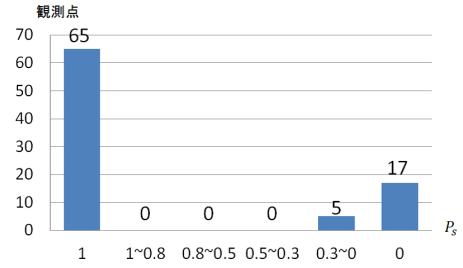

図 16　プライバシ侵害データを含む観測点の空間的な確からしさ

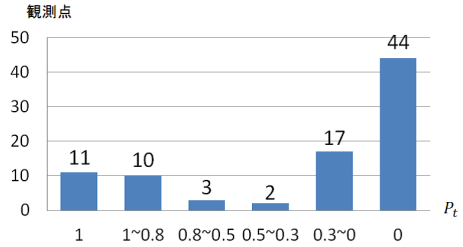

図 17　プライバシ侵害データを含む観測点の時間的な確からしさ

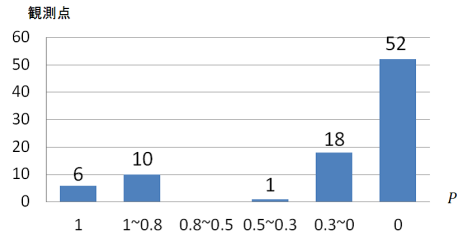

図 18　プライバシ侵害データを含む観測点の信頼性

5.3.2　計算結果の抽出

評価データの中に，プライバシ侵害データを含む 87 個の観測点の空間的な確からしさ，時間的な確からしさ，信頼性それぞれを抽出して，結果は図 16，図 17，図 18 に示す．

5.3.3　信頼率

プライバシ侵害データを含む観測点の信頼率は表 7 に示す．空間的な確からしさのみを用いた場合，プライバシ侵害データの信頼率は 74%以上になった．実データにより，1 つの基地局しかない地点は多く存在する．これらの地点には空間的な確からしさがプライバシ保護に効かないため，空間的な確からしさだけで判断する場合，信頼率が高くなった．信頼性に基づくプライバシ侵害データの信頼率は約 18%になる．つまり，プライバシ侵害データの検出率は約 82%になることが分かった．

表 7　信頼率

	空間的な確からしさ	時間的な確からしさ	信頼性
信頼率	74.71%	27.59%	18.39%

5.4　考察

検証実験の結果 (表 7) により，本稿で提案したユーザの信頼性を判断するアルゴリズムがプライバシ侵害問題をあ

る程度で解決できることを確認した．一方，表 6 により，評価データ全体では，信頼性は低くなっている．そのため，ユーザの利用目的により，適当に閾値を変更する必要がある．

計算時間について，本実験は 1 つの観測点は約 1 秒かかることが分かった．ただし，データベースの規模により，計算時間は変わるはずである．そのため，状況に応じて，動作環境を向上する必要がある．

6. おわりに

本稿では，無線 LAN 位置推定におけるプライバシ保護のため，ユーザ (または端末) が推定位置にいる空間的な確からしさと時間的な確からしさの両方を考慮し，信頼性を判断するアルゴリズムを提案した．評価実験により，信頼性に基づくプライバシ侵害データの検出率は 82%になった．計算時間は動作環境とデータベースの規模に依存するが，本実験で 1 つの観測点が約 1 秒かかることも分かった．以上から，本手法は高い確率で無線 LAN におけるプライバシ問題を解決できることを確認した．

今回の評価実験で使用した評価データ量は一部のみであるため，今後大規模のデータに適用することを考えている．さらに，様々な状況に対応するため，攻撃実験も考えている．

参考文献

[1] Anthony LaMarca, Jeffrey Hightower, Ian Smith, Sunny Consolvo: Self-Mapping in 802.11 Location Systems,In Proceedings of the Seventh International Conference on Ubiqutous Computing 2005,pp.87-104.

[2] Julian Lategahn, Frank Kuenemund, Christof Roehrig: Mobile Robot Localization Using WLAN,Odometry and Gyroscope Data, International Journal of Computing, Vol.9,Issue 1,pp.22-30(2010)

[3] Nils Ole Tippenhauer, Kasper Bonne Rasmussen, Christina Popper, and Srdjan Capkun: Attacks on Public WLAN-based Positioning Systems, Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services (MobiSys)(2009)

[4] Varela, F., Sebastiao, P., Correia, A., Cercas, F., Velez, F.J., Robalo, D.and Rodrigues, A.: Unified Propagation Model for Wi-Fi, UMTS and WiMAX Planning in Mixed Scenarios, in Proc. of PIMRC' 10-21st IEEE International Symposium on Personal Indoor, and Mobile Radio Communications, Istanbul,Turkey(2010).

[5] Varela, F., Sebastiao, P., Correia, A., Cercas, F., Velez, F.J., Robalo, D. and Rodrigues, A.: Validation of the Unified Propagation Model for Wi-Fi, UMTS and WiMAX Planning, in Proc. of PIMRC' 10-21st IEEE International Symposium on Personal Indoor, and Mobile Radio Communications, Istanbul, Turkey(2010).

[6] Muzaiyanah Hidayab, Abdul Halim Ali, Khairul Bariah Abas Azmi: Wifi Signal Propagation at 2.4 GHz, Microwave Conference, 2009. APMC 2009. Asia Pacific(2009).

[7] Sebastian Thrun, Wolfram Burgard, Dieter Fox: *Probabilistic Robotics*, The MIT Press(2005).

[8] Google : Greater choice for wireless access point owners, 入手先 ⟨http://googleblog.blogspot.jp/2011/11/greater-choice-for-wireless-access.html⟩ (2012.11.02).

[9] 河口信夫 : Locky.jp : 無線 LAN を用いた位置情報ポータルとその応用，ヒューマンインタフェース学会誌，Vol.10,No.1,pp.15-20(2008).

[10] 梶 克彦, 河口 信夫: indoor.Locky: UGC を利用した無線 LAN 屋内位置情報基盤，情報処理学会論文誌，Vol.52,No.12(2011) V1-230(2010).

[11] 中西 健一, 高汐 一紀，中澤 仁，徳田 英幸: 位置情報粒度の動的変更によるプライバシ保護機構，第 7 回プログラミングおよび応用のシステムに関するワークショップ（SPA2004）論文集，pp.50-60(2004).

[12] Locky.jp : 無線 LAN を用いた位置情報・測位に関するポータルサイト，入手先 ⟨http://locky.jp/⟩ (2012.11.02).

[13] 新田 優介, 大野 成義: 無線 LAN のアクセスポイントを利用した位置推定方法の比較検討，職業能力開発総合大学紀要,No41-A,(2012)

[14] 何 韜，梶 克彦，河口 信夫 : 位置推定のための健全性維持手法の大規模無線 LAN データベースへの適応，モバイルマルチメディア通信研究会，MoMuC2011-29，2011.11

[15] プローブ自転車による自転車歩行者道のバリア調査法，土木計画学研究・論文集，Vol.22 2005.10

[16] 米川 隆 : 市街地走行の現実感を目指したドライビングシミュレータの開発，JARI ITS セミナー 2009.9