無線LANを利用した移動体位置推定法とそのセキュリティに関する研究

伊沢，亮一

(Degree)
博士（工学）
(Date of Degree)
2012-03-25
(Resource Type)
doctoral thesis
(Report Number)
甲5501
(URL)
https://hdl.handle.net/20.500.14094/D1005501

（別紙１）　　論文審査の結果の要旨

氏名	伊沢　亮一		
論文題目	無線 LAN を利用した移動体位置推定法とそのセキュリティに関する研究		
審査委員	区　分	職　名	氏　　名
	主　査	教　授	森井　昌克
	副　査	教　授	八坂　保能
	副　査	教　授	小澤　誠一
	副　査		印
	副　査		印

要　　旨

近年，ノート PC やスマートフォンなどのモバイル端末の普及に伴い，ナビゲーションシステムなどの位置情報サービスが盛んに開発されている。ユーザは位置情報サービスを利用することで周辺の店舗の情報や目的地までの経路を取得することができる。位置情報サービスの要素技術として，ユーザの位置を推定する方法，安全な認証・通信プロトコル，サービスに関する情報を作成するプログラムなどが挙げられる。より良い位置情報サービス構築のために要素技術ごとに課題があり，それぞれに対して研究がなされている。本論文では位置情報サービスの構築を目的とし，要素技術のうち，ユーザの位置推定法と認証・通信プロトコルについて課題を議論し，その課題を解決する方法を提案している。

本論文の構成は以下のとおりである。

第１章は緒論である。ユーザの位置推定法，認証・通信プロトコルに関する研究背景を述べた後，それぞれに関する既存方式の概要と課題を述べている。さらに，本論文で提案する方式の発想と着眼点について要約している。

第２章では位置情報サービスの環境および手順を説明した後，基礎知識について述べている。位置推定法の基礎知識として，環境が電界強度に与える影響を説明してから，いくつかの基本となる方式の説明，比較を行っている。提案方式および従来方式は基本となる方式のいずれかに属する。匿名認証方式の基礎知識として，Zhu らの方式の目標やプロトコルを説明してから，He らの方式を説明している。He らの方式はユーザとサーバの二者による匿名認証方式であるが，ユーザは公開鍵暗号を使用する点が Zhu らの方式と異なる。Zhu らの方式と He らの方式を比較することで，Zhu らの方式の利点および欠点を明確に与えている。

第３章では電界強度データベースと判別分析，測位対象の移動状態遷移モデルを利用する方法を提案している。位置情報サービスではユーザの位置情報をもとにサービスを提供するため，精度の高い位置推定法が必要となる。一般的な位置推定法として，GPS（Global Positioning System）が利用されるが，地下街などの屋内空間では GPS 信号が受信できず位置推定ができない。そこで，屋内空間における位置推定法が求められている。既に設置されている通信インフラとしての無線 LAN の利用が考えられるが，一般には精度の高い位置推定を行うことは困難である。その一因としては，反射波や障害物の影響等が無線 LAN 基地局からの受信電界強度を大きく揺るがすことにあると考えられる。本論文では電界強度データベースと測位端末の移動状態遷移モデルを用い，受信電界強度の揺らぎから受ける影響を減少させ得ることで精度を向上させている。電界強度データベースでは位置推定を行う場所の電界強度をデータベース化し，移動状態遷移モデルでは地下街での人の動きを予測することで精度の向上を実現している。提案方式は 1m の誤差で位置推定が可能である。GPS の利用が困難な屋内において本方式は有効であるといえ，特に人の移動が直線的で自由度が制限される地下街において効果的であると考えられる。

第４章では有効期限が設定可能な匿名認証方式を提案している。既存方式として Kang らの方式が挙げられるが，安全性に問題があり有効期限に関して厳密に与えられていない。具体的には，同一の HA に所属する MU 間で匿名性が確保できない。また，有効期限に関しても，有効期限後に MU のモバイル端末から秘密情報が取り出せないことを仮定しているだけであって目的を達成しているとは言い難い。それらを改善するために，有効期限が設定できる安全な方式を提案している。性能に関しては，Kang らの方式と比べ MU の記憶容量と計算量，通信量が多少増加するが，安全な匿名認証を実現するために必要なコストであることが示されている。課金型などの位置情報サービスでは MU に対して有効期限を設定する必要があり，提案方式はこのようなサービスの構築に貢献できる。

氏名	伊沢　亮一

第５章ではユーザの秘密情報漏洩に耐性がある匿名認証方式を提案している。既存方式として Cui らの方式と Lee らの方式が挙げられるがそれぞれ安全性に課題がある。Cui らの方式では MU が生成するログインメッセージに固定値が含まれており，FA が MU を追跡できるという課題がある。Lee らの方式ではパスワード推測攻撃に耐性がなく，HA が認証データベースを保持しているという課題がある。提案方式はこれらの課題を全て解決している。従来方式に比べ，MU や HA の演算回数は多少増えるものの，安全な認証を実現するために必要な処理である。提案方式を用いることで，不正アクセスやマルウェア等により MU のモバイル端末から秘密情報が漏洩したとしても，サービスの不正利用を防ぐことができる。

第６章は結論である。３章から５章の概要および結果を要約している。

以上のように本研究はユーザの位置推定法と匿名認証方式について研究したものであり，今後より一層需要が増えると予想される位置情報サービスの開発に大きく貢献できる重要な知見を得たものとして価値ある集積であると認める。よって，学位申請者の伊沢 亮一は，博士（工学）の学位を得る資格があると認める。

(別紙様式 3)

論文内容の要旨

氏　　名　伊沢　亮一

専　　攻　情報・電子科学専攻

論文題目（外国語の場合は，その和訳を併記すること。）

無線 LAN を利用した移動体位置推定法とそのセキュリティに関する研究

指導教員　森井　昌克

（注）2，000 字～4，000 字でまとめること。

近年，ノート PC やスマートフォンなどのモバイル端末の普及に伴い，ナビゲーションシステムなどの位置情報サービスが盛んに開発されている．ユーザは位置情報サービスを利用することで周辺の店舗の情報や目的地までの経路を取得することができる．

ユーザがサービスを受けるまでの流れは次のようになる．ユーザはモバイル端末により自身の位置を推定し，ID とログインメッセージ，位置情報をインターネット経由でサーバに送信する．ここで，ログインメッセージとはサーバがユーザを認証するための情報である．サーバは正規のユーザであることを認証し，周辺の店舗の情報などのサービスに関する情報を作成する．サーバがその情報をユーザに送信することでサービスが提供される．このような位置情報サービスの要素技術として，ユーザの位置を推定する方法，安全な認証・通信プロトコル，サービスに関する情報を作成するプログラムなどが挙げられる．より良い位置情報サービス構築のために要素技術ごとに課題があり，それぞれに対して研究がなされている．本研究では位置情報サービスの構築を目的とし，要素技術のうち，ユーザの位置推定法と認証・通信プロトコルに着目する．具体的な研究テーマとして，以下の 3 つに分けられる．下記の（1）がユーザの位置を推定する方法に関するテーマであり，（2）と（3）が安全な認証・通信プロトコルに関するテーマである．

（1）屋内空間における精度の高い位置推定法
（2）有効期限の設定が可能な匿名認証方式
（3）ユーザの秘密情報漏洩に耐性がある匿名認証方式

（1）では，屋内空間に適した精度の高い位置推定法を提案する．位置情報サービスはユーザの位置情報をもとにサービスを提供するため，精度の高い位置推定法が必要となる．一般的な位置推定法では，GPS（Global Positioning System）が利用されるが，地下街などの屋内空間では GPS 信号が受信できず位置推定ができない．そこで，屋内空間における位置推定法が求められている．既に設置されている通信インフラとしての無線 LAN の利用が考えられるが，一般には精度の高い位置推定を行うことは困難である．その一因としては，反射波や障害物の影響等が無線 LAN 基地局からの受信電界強度を大きく揺るがすことにあると考えられる．本論文では電界強度データベースと測位端末の移動状態遷移モデルを用い，受信電界強度の揺らぎから受ける影響を減少させ得ることで精度を向上させることを試みる．電界強度データベースでは位置推定を行う場所の電界強度をデータベース化し，移動状態遷移モデルでは地下街での人の動きを予測することで精度の向上を実現している．提案方式は 1m の誤差で位置推定が可能である．GPS の利用が困難な屋内において本方式は有効であり，特に人の移動が直線的で自由度が制限される地下街において効果的であると考えられる．

（2）および（3）では，それぞれ匿名認証方式を提案する．本研究では無線 LAN によりユーザとサーバが通信することを想定している．有線通信と異なり，無線通信は電波が届く範囲全てに通信データが送信されるため，盗聴や通信相手のなりすましなどのインシデントが容易に発生する．このようなインシデントを防ぐためには双方向認証と暗号化通信が基本となる．双方向認証によりユーザとサーバが互いに認証することでなりすましを防ぎ，暗号化通信により盗聴を防ぐ．

本研究ではより安全な通信のためにユーザの匿名性の確保を目的とする．位置情報サービスでは，ユーザが ID と位置情報をサーバに送信するため，ユーザの現在位置や移動履歴をサーバに知られてしまう．プライバシ保護の観点からユーザの匿名性を確保した上で認証・暗号化通信が可能な方式（匿名認証方式）が求められている．匿名認証方式では，公開鍵暗号を利用する方法が一般的であるが計算量が大きいことが課題として挙げられる．そこで，Zhu-Ma らはユーザとサーバに加え，ホームエージェントを導入することでユーザが公開鍵暗号を利用しない方式を提案した．サーバの代わりにホームエージェントがユーザを認証することで匿名認証を実現している．しかしながら，Zhu-Ma らの方式は脆弱性が指摘されており，改良方式が提案されている．

本論文では 2 つの匿名認証方式を提案する．（2）の方式として，有効期限の設定が可能な匿名認証方式を提案する．匿名認証ではサーバがユーザを特定できないため，ユーザを特定することなく有効期限を判定する仕組みを与える．有効期限は課金型の位置情報サービスなどで必要となる．（3）の方式では，ユーザの秘密情報漏洩に耐性がある匿名認証方式を提案する．近年，不正アクセスやマルウェアの被害が増加している．これらの被害により，モバイル端末から秘密情報が漏洩したとしても，サービスの不正利用を防ぐことができる．（2）の既存方式として Kang-Rhee-Choi らの方式が挙げられる．Kang-Rhee-Choi らは安全な匿名認証に加え，ユーザに有効期限を与えることを目的とし方式を提案した．しかしながら，Kang-Rhee-Choi らの方式はホームエージェントに所属するユーザ間で匿名性が確保できない．有効期限に関しても，有効期限後に秘密情報が取り出せないモバイル端末をユーザに与えているだけで，厳密に有効期限を設定できているとは言い難い．本論文では有効期限が設定できる安全な匿名認証を提案する．ここで，安全な方式とはホームエージェントに所属するユーザ間においても匿名性が確保できる方式のことを意味する．（3）の既存方式として Cui-Qin らの方式と Lee-Kwon らの方式が挙げられる．ユーザのモバイル端末から秘密情報が漏洩したとしても，悪意のある第三者がユーザになりすますことを防ぐことができる．しかしながら，Cui-Qin らの方式はログインメッセージに固定値が含まれており，これをもとにサーバがユーザの通信を追跡することができる．Lee-Kwon らの方式では安全性がユーザの設定するパスワードに依存するといった課題がある．本論文では，これら 2 つの欠点を改善した秘密情報の漏洩に耐性がある方式を提案する．

本論文の構成は次の通りである．1 章では緒論を述べる．緒論では本要旨を詳細に述べ，研究背景や提案方式の位置付けを明確に与える．2 章では位置情報サービスの環境および手順を述べた後，位置推定法および匿名認証方式の基礎知識を述べる．位置推定法の基礎知識として，環境が電界強度に与える影響といくつかの基本となる方式の説明，比較を行う．提案方式および従来方式は基本となる方式のいずれかに属する．匿名認証方式の基礎知識として，Zhu らの方式の目標やプロトコルを説明してから，He らの方式を説明する．He らの方式はユーザとサーバの二者による匿名認証方式である．ただし，ユーザは公開鍵暗号を使用する．Zhu らの方式と He らの方式を比較することで，Zhu らの方式の利点および欠点を明確にする．3 章は研究テーマ（1）の内容で構成される．従来の位置推定法を説明した後，提案方式の概要を述べ従来方式との差異を明確にする．次にデータベースと判別分析による位置推定法（提案方式 1）の詳細を与え，ユーザの移動状態に関するモデルを利用した方式（提案方式 2）の詳細を与える．評価実験では直線の通路において，提案方式 1 と提案方式 2，Kushki らの方式を比較し提案方式 2 の有効性を示す．提案方式では 28.0 ×2.4m の通路において誤差 1m の精度で位置推定が可能である．4 章は研究テーマ（2）の内容で構成される．まず匿名認証方式が利用される環境および目的を説明する．次に，従来方式として Kang らの方式のプロトコルを述べた後，脆弱性を指摘する．その脆弱性を踏まえた上で，有効期限の設定が可能な匿名認証方式を提案し，安全性の検証および性能評価を行う．5 章は研究テーマ（3）の内容で構成される．従来方式として Wu らの方式，Cui らの方式，Lee らの方式の脆弱性を指摘する．それらの脆弱性を踏まえた上で，ユーザの秘密情報漏洩に耐性がある匿名認証方式を提案し，安全性の検証および性能評価を行う．6 章で結論を述べる．