様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年　 6 月　 17 日現在

機関番号：20103
研究種目：若手研究（B）
研究期間：2010 年～2012 年
課題番号：22700071
研究課題名（和文）　ユビキタスネットワークにおけるプライバシ保護手法に関する研究

研究課題名（英文）　Study on privacy protection method in ubiquitous network

研究代表者
中村　嘉隆（NAKAMURA YOSHITAKA）
公立はこだて未来大学・システム情報科学部・助教
研究者番号：40452528

研究成果の概要（和文）：
商業地域において，ユーザの位置情報などを用いたコンテクストアウェアなサービスの需要が大きくなっている．このとき，ユーザが自分の位置情報を完全にトレースされてしまうことはプライバシ的に問題があり，サービスのための積極的な情報提供がされない可能性がある．また，比較的小さな店からなるショッピングモールではコンテクストアウェアなサービスの提供基盤を店が自前で構築するのはコストが高すぎるため，モール全体で共有基盤を構築してサービスの提供を行うことが考えられるが，このサービスを自店の顧客統計データにもとに，条件を設定しながら行うような場合，共有基盤を通じて他店に顧客データが漏れてしまう可能性があり，こちらも積極的な利用がためらわれる原因となる．そこで本研究では，ユーザのコンテクスト情報，サービス提供者のサービス提供条件をそれぞれ外部に秘匿したまま，コンテクストに応じたサービスを提供できる基盤の設計を行った．また，ユーザのプライバシを確保したままユーザの動線をサービスプロバイダに対して提供するための計測手法についても提案を行った．

研究成果の概要（英文）：
In commercial districts, the demand for the context-aware services using such as the location information of the users is increased. However, there is a possibility that the information for services may not be reported positively, since it is a problem on users' privacy that users are traced their location information completely. In addition, from the point of view of cost, if the service delivery infrastructure is shared for the context-aware service by the whole shopping mall, there are risks that customer data leaks to other stores through this shared infrastructure. In this study, we proposed the foundation that can provide the context-aware service while concealing the context information of each user, the service delivery conditions of the service provider to the others. And we also proposed the measurement technique to provide the flow line of users to the service provider with protecting privacies of users.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	900,000	270,000	1,170,000
2011 年度	900,000	270,000	1,170,000
2012 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	2,800,000	840,000	3,640,000

研究分野：計算機システム・ネットワーク
科研費の分科・細目：ネットワークセキュリティ技術
キーワード：モバイルネットワーク

１．研究開始当初の背景

有線・無線通信技術の発展などに伴い，あらゆる時間・地点でネットワークに接続できるユビキタス社会の到来が期待されている．このユビキタス社会を実現するための重要な技術としてセンサネットワークが注目されている．センサネットワークでは，収集した情報を直接データとして扱うことが多く，利用者のプライバシを考慮した場合，扱い方に注意する必要がある．一方，センサネットワークを構成するセンサ端末は一般に低性能であるため，暗号技術など従来のプライバシ保護技術における負荷の高い計算を行なうことが困難である．また，異なる種類のセンサネットワークは異なる目的のために展開される可能性があるため，それぞれについて保護すべきプライバシは動的に変化する可能性がある．例えば，そのため，センサネットワーク向けに利用者のプライバシを保護するための効果的な手法を開発することが必要となっている．

センサネットワークにおけるプライバシ保護技術には，暗号技術・DoS（Denial of Service）攻撃等からのネットワークサービス保護技術・コンテクスト情報管理技術の 3 つに大別される．ここで，コンテクスト情報とはユーザの状況を表す情報，すなわち時刻・位置・行動（加速度）・周囲の環境（温度，気圧，照度）等のことを表す．これらのプライバシ保護技術のうち，暗号技術についてはこれまでに多くの研究がなされており，また，ネットワークサービス保護技術については，各攻撃型に応じた保護技術が提案されてきている．

そこで，最も重要となると考えられるコンテクスト情報を用いたユビキタスサービス適用時において，適切なプライバシ保護を実現することは，ユビキタス社会において重要な問題であると考え，本研究を着想するに至った．

２．研究の目的

本研究課題では，コンテクスト情報におけるプライバシ保護に着目する．現状のサービス提供時に用いられているセンサネットワークなどのネットワークでは，センサの盗難や盗聴が比較的容易であり，センサで取得したコンテクスト情報によってプライバシ情報を類推することが可能であったりするなど，プライバシ保護上の問題点がある．そこで，コンテクスト情報を生データのままではなく何らかの変形を加えて処理・送受信を行うことで，例えば，ユーザ・サービスプロバイダ間で時刻やユーザの位置，サービスプロバイダのサービス提供領域，サービス提供時間帯，サービス提供グループについて，互いに知らせあうことなくサービスに必要な情報のみを共有するプライバシ保護手法を提案した．

本課題では，直接通信を行うユーザおよびサービスプロバイダそれぞれに対してさえ，プライバシ情報を公開しないままに通信を行うため，外部からの盗聴に対するプライバシ情報の保護はもとより，当該通信者であるユーザ，サービスプロバイダ同士でプライバシ情報の保護が可能であるという点で，新規性があると考えられる．また，さまざまなタイプの情報に対応することで，より情報の安全性を高めることに寄与するものと考えている．

３．研究の方法

プライバシ保護を考慮した通信を実現させるために，例えばユーザ・サービスプロバイダ間で時刻やユーザの位置，サービスプロバイダのサービス提供領域，サービス提供時間帯，サービス提供グループについて，互いに知らせあうことなくサービスに必要な情報を提供する必要がある．

そこで，ユーザおよびサービスプロバイダそれぞれの位置情報について，互いに相手に知らせないままに互いの位置関係を把握するためのプロトコルの設計を行った．サービス提供領域の境界，およびユーザの位置情報をベクトルで表現し，紛失通信（Oblivious Transfer）と呼ばれる暗号プロトコルの技法を用いて，正確な位置情報を共有することなく，互いの位置関係のみの結果をユーザ・サーバプロバイダ間で共有させる．

ある端末 S がサービスプロバイダのサービス領域 A 内に入ったときの位置座標を $p(\alpha,\beta)$ とする（図 1）．このとき各端末は GPS などのセンサからこの位置座標を取得できるものとする．また，各サービスプロバイダはサービス領域 A の境界線を n 角形に近似し，その地点の位置座標 (x,y) から，(x,y) がサービス領域の境界線上であるときに $f_i(x,y) = 0\ (i \in 1,\ldots,n)$ で表すことができるとする（図 2）．ここでサービスプロバイダも位置情報を取得することができるものとする．このとき，位置 (α,β) にある端末 S がサービス領域 A の内部にあることを，各 $f_i(\alpha,\beta) = 0\ (i$

$\in$ 1,…,n) の計算結果から判別する．ここで，$f_i(x,y)$ および(α,β)はサービスプロバイダ，およびユーザ端末のプライバシ情報にあたるため，この情報の交換に紛失通信を用いて，お互いに $f_i(x,y)$ および(α,β)それぞれの情報を相手に知らせないまま，すなわちユーザ・サービスプロバイダ間で共有しないまま，計算結果 $f_i(\alpha,\beta)$ $(i \in 1,\ldots,n)$のみを共有させ，サービスの提供に用いるようにする．

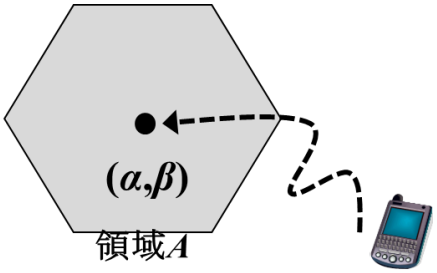

図1

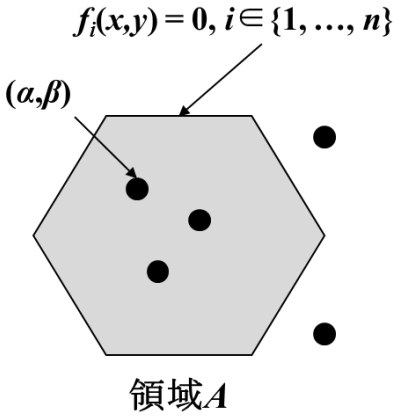

図2

具体的な計算処理は以下の通りである．まず，領域 A を図 1 のような六角形の領域であると想定し，左端と右端の頂点で上下に分割する（図 3）．$f_i(x,y)$は上部・下部それぞれの境界線を表すので，この方程式にユーザ端末の位置 $p(\alpha,\beta)$を代入したとき，上部では負の値，下部では正の値が返ってくれば，点(α,β)は領域 A に含まれることになる．

次に，プライバシ情報である $f_i(x,y)$，(α,β)を秘匿しつつ通信を行う．暗号プロトコルの一種である紛失通信手法を用い，サービスプロバイダ側はサービス領域境界 $f_i(x,y)$ $(i \in 1,\ldots,n)$にランダムな正の整数 v_i $(i \in 1,\ldots,n)$を加えた $f_i(x,y)+v_i$ $(i \in 1,\ldots,n)$をユーザに公開する．領域 A 各辺に乱数が加えられているために，ユーザは正確な境界線を知ることができない．一方，ユーザ側は与えられた $f_i(x,y)+v_i$ $(i \in 1,\ldots,n)$に(α,β)を代入し，計算結果 $u_i = f_i(\alpha,\beta)+v_i$ $(i \in 1,\ldots,n)$を得る．この

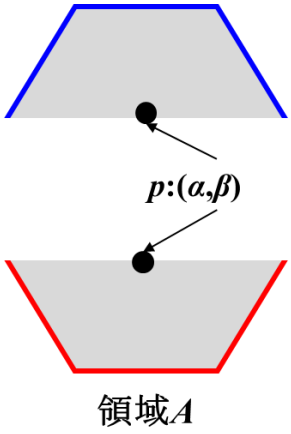

図3

u_i $(i \in 1,\ldots,n)$をサービスプロバイダに対し公開する．このとき，u_i $(i \in 1,\ldots,n)$にはユーザの位置座標情報(α,β)が含まれていない．サービスプロバイダはこの v_i および u_i を用いてサービス領域内にユーザが存在するかどうかを判定する．全ての $i \in 1,\ldots,n$ において $u_i \geqq v_i$ が成立するときのみユーザがサービス領域 A 内に存在することになる．

また，提供されるユビキタスサービスには人流の動線情報を解析し，その解析結果に基づいて提供方針が決定されるものも想定される．また，人流そのものを制御するサービスも提供されうる．このような場合，カメラによる動画像によって歩行者を認識するなどの手法が考えられるが，各ユーザの行動がユーザの許可を得ないまま記録されることになり，よりプライバシに配慮した人流情報取得手法が求められる．本研究ではレーザ光を高速に回転させながらその反射を記録することで，対象物までの距離を計測することができるスキャナ式レンジセンサを利用する．複数のスキャナ式レンジセンサによって捕捉された物体の時系列変動パターンから，人間の歩行パターンを推定し（図 4），人流モデルを生成する手法を提案した．スキャナ式レンジセンサは，障害物越しの物体までの距離計測が不可能であるなど，計測範囲の見晴らしの影響を強く受けるため，計測領域内の全ての歩行者の動向を完全に捕捉することが難しい．そこで提案する人流モデル化手法では，計測領域をいくつかの区画に分割し，個々の歩行者の位置データではなく，区画毎の人口密度に注目し，人口密度の大小およびその増減から歩行者が通過したであろう経路を予測し，人流データを作成する（図 5）．これによって，計測領域内の全ての歩行者の移動パターンを完全には捕捉できていない不完全なデータであっても，人流を流量と流れの向きをもったフロー形式で表し，モデル化することを可能にしている．

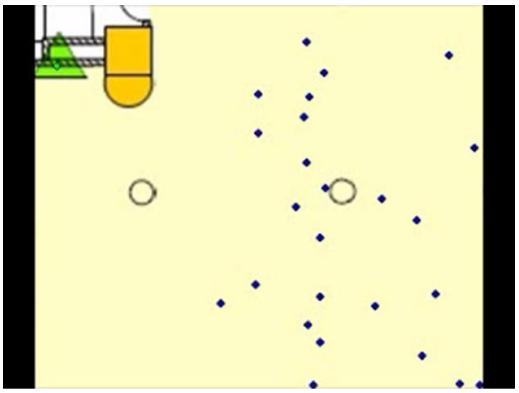

図4

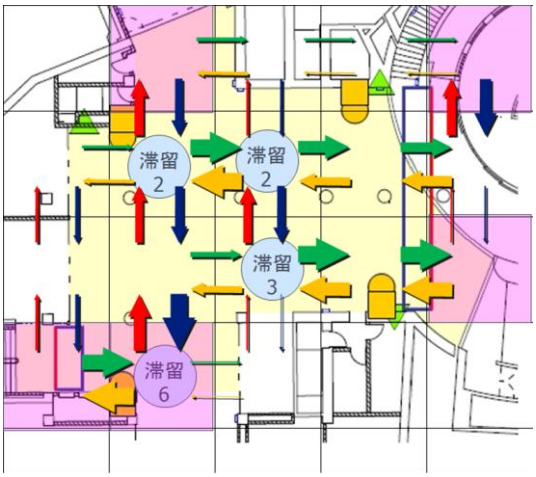

図5

４．研究成果

ユーザおよびサービスプロバイダそれぞれの位置情報について，互いに相手に知らせないままに互いの位置関係を把握するためのプロトコルの設計を行った．このプロトコルではサービスプロバイダはサービス領域の境界線を n 角形に近似し，ある端末の位置座標がサービスの n 個の境界線に対してどちら側にいるかを，お互いの情報を開示しないまま，その判定結果のみを紛失通信を用いて交換することに成功した．また，提案プロトコルに対して，より広範囲のプライバシ情報を秘匿するための改良をすすめ，ユーザおよびサービスプロバイダの持つサービス情報（それぞれの位置，時間，行動コンテクスト情報）を秘匿しつつ共有する手法の検討を行った．

また，ユーザのコンテクスト情報を秘匿したまま，各ユーザの行動における動線などの集積データをサービスプロバイダに提供する手法は，査読付き国内会議及び査読付き国際会議に採録され，査読付き英文論文誌に掲載された．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１件）

① Yoshitaka Nakamura, Yusuke Wada, Teruo Higashino and Osamu Takahashi, "A Method for Modeling of Pedestrian Flow in the Space with Obstacles using Laser Range Scanners," International Journal of Informatics Society (IJIS), Vol.4, No.1, pp.41-49, 2012. 査読有

〔学会発表〕（計３件）

① Yoshitaka Nakamura, Yusuke Wada, Teruo Higashino and Osamu Takahashi, "A Method for Modeling of Pedestrian Flow in the Obstacle Space using Laser Range Scanners," Proceedings of the International Workshop on Informatics (IWIN2011), pp.54-61, 2011. 査読有

② 三浦愛美，中村嘉隆，白石陽，高橋修，"MANET における信頼性を考慮した証拠収集手法の提案," マルチメディア，分散，協調とモバイル (DICOMO2011) シンポジウム論文集, pp.978-986, 2011. 査読有

③ 和田悠佑，中村嘉隆，東野輝夫，"障害物の存在する空間におけるレンジスキャナを用いた人流モデル化手法の提案," マルチメディア，分散，協調とモバイル (DICOMO2011) シンポジウム論文集，pp.1183-1192, 2011. 査読有

６．研究組織

(1)研究代表者

中村　嘉隆（NAKAMURA YOSHITAKA）
公立はこだて未来大学・システム情報科学部・助教
研究者番号：40452528