マルチメディア通信と分散処理 108－3
（２００２．６．６）

地理位置情報システムの実装と評価

渡辺恭人[†] 竹内奏吾[††]
寺岡文男[†††] 村井純[†††]

インターネットにおいて物理的空間を移動するホスト（移動体）の地理位置情報を管理する仕組みとして，我々は，地理位置情報システム (Geographical Location Information (GLI)System) を提案している．地理位置情報システムでは，移動体の識別子と地理位置情報（緯度・経度・高度）を登録し，識別子と地理位置情報の双方から，移動体を検索することができる．サーバの分散管理による大規模性，プライバシ保護を実現している，本稿では，GLI プライバシ保護機能を含んだ GLI システムの実装と，2001 年 3 月に横浜で行われたプローブ情報システム実験のデータを使用した本システムの動作検証について述べる．

The implimentation and evaludation of Geographical Location Information System

Yasuhito Watanabe,[†] Sohgo Takeuchi,[††] Fumio Teraoka[†††] and Jun Murai[†††]

We propose the Geographical Location Information (GLI) System, that manages geographical location information of mobile entities. In this system, every mobile entity register its identifier and its geographical location information (longitude, latitude, altitude). Users can look-up mobile entities location using their identifiers as a search key, and vice versa. Also, distributed management of servers and protection of mobile entities' privacy are supported.

In this paper, we implemented the function of privacy protection to expand the GLI System. We test and test the system using data of the IPCar experimentation held in Yokohama City, March 2001.

1. はじめに

インターネットに接続されるものは計算機だけでなく，車や様々なセンサーデバイスなど多様になっている．それらは，多数で，現実の空間において移動，遍在している．このような移動体や移動体が持つ情報を有効に取り扱うためには，移動体の地理的な位置を管理することが重要になってきている．カーナビゲーションにおいては自車がどこにいて，周囲に何があるかという，位置に依存した情報提供を行い，携帯電話でも同様のサービスが存在する．また，多数の移動体から情報を収集し，その情報を活用する例もある [1)]．

インターネットにおいて物理的空間を移動するホスト（移動体）の地理位置情報を管理する仕組みとして，我々は，地理位置情報システム (GLI System) を提案し開発している．本システムでは管理対象となる移動体の識別子と緯度・経度・高度で代表される地理位置情報のみを登録し，その両者を鍵とした検索機構を提供する．一つは，識別子を鍵とした検索 (正引き検索) であり，もう一つは地理位置情報を鍵とした検索 (逆引き検索) である．また，プライバシ保護機構を持っており，信頼関係者間において秘密の識別子，時刻情報を共有することにより，第三者には理解できない Hashed ID(HID) を識別子として登録する．また，時刻によって HID が変化することにより，追跡を防止する．但し，地理位置情報は隠蔽しないので，第三者は検索により移動体の個数と位置といった分布統計情報を取得できる．

本稿では，本システムの実装と評価を行った．また，サンプルアプリケーションを作成し，2001 年 3 月に横浜において行われたプローブ情報システム実験のデータを使用して，本システムの動作検証について述べる．

† 慶應義塾大学 SFC 研究所
SFC Laboratory, Keio University
†† （株）ソニーコンピュータサイエンス研究所
Sony Computer Science Laboratories, Inc.
††† 慶應義塾大学
Keio University

2. 地理位置情報システムの概要

地理位置情報システム（GLI: Geographical Location Information System）[2)3)] は，現実世界を移動する移動体を対象とし，その識別子と地理位置情報の登録・検索機能を持つミドルウェアである．移動体はサーバに地理位置情報と識別子を登録し，クライアントは，識別子や地理位置情報を鍵とした検索要求をサーバに送信することにより，移動体を検索することができる．GLI システムにおける地理位置情報とは緯度・経度・高度であり，移動体識別子とはホストの識別子である．識別子をオープンに登録する場合は，FQDN(Fully Qualified Domain Name) で記述されるホスト名を使用する．HID(Hashed ID) を使用することでプライバシを保護できる．また，文献 [3)] ではサーバの階層化による分散管理を実現しており，地球規模での分散管理が可能となっている．

2.1 検索の種類

GLI システムは，以下の 2 種類の検索機能を提供する．

- 正引き検索
  移動体の識別子を鍵とし，その移動体の位置情報を返す．例えば，移動体の識別子を指定して検索し，その地理位置情報 (北緯 35 度 18 分 15 秒，東経 139 度 30 分 40 秒) を得る．
- 逆引き検索
  地理的な領域を指定し，その領域に存在する移動体の識別子，位置情報の集合を返す．GLI システムでは，範囲検索/最近接検索の 2 種の逆引き検索を持つ．(図 1).

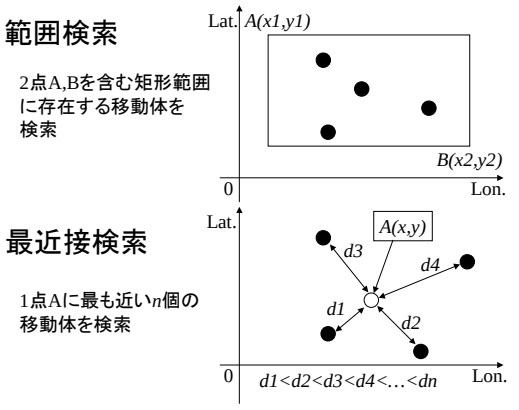


図 1 範囲検索と最近隣検索

2.2 セキュリティ上の脅威とプライバシ保護

GLI サーバ群と移動体および検索者はインターネットを介して通信する．GLI システムでのプライバシ保護を考える上で，以下の 2 つの前提を置く．1 つは，インターネットでの通信では基本的にセキュリティが考慮されていないことである．もう 1 つは GLI サーバは不正を行わないということである．また，移動体にとって，信頼関係にある検索者と信頼関係のない検索者（第三者）という区別があるものとする．このような前提条件のもと GLI システムはプライバシ保護について，以下のような目標を持つ．

- 移動体特定の防止
- 追跡の防止
- 偽の移動体情報登録防止
- データベース盗難の防止
- 盗聴・改竄の防止

ある移動体と信頼関係にあるクライアントだけが生成し理解でき，それ以外の第三者にとっては無意味な文字列であり，かつ，真の識別子に復元不可能とすることで移動体の特定を防ぎ，プライバシを保護する．

ある移動体と信頼関係にあるクライアントだけが生成し理解できる HID は，その両者の間で共有される秘密の識別子を特定のハッシュ関数に通すことで生成される．ハッシュ関数の一方向性を利用し，HID が公開されても真の識別子を得ることを不可能にしている．但し，常に同じ HID を利用し続けると，追跡が可能となる．これを防ぐために，HID を定期的に変更するようにする．新たな通信をせずに HID を変化させるために，時刻情報をハッシュ関数の入力値に加える．実際には，基準時刻と HID を変更する間隔を入力する．HID の生成には，鍵付きハッシュ関数（HMAC: Keyed Hashing for Message Authentication）[6)] を使用する．

登録サーバの導入による移動体認証

移動体を認証し，移動体の情報は登録せずにデータベースを持つ HID サーバに転送を行う登録サーバを導入する．データベースを持つ HID サーバは登録 HID によって固定されないため，認証が困難になる．登録サーバを導入することにより，移動体は常に同じ登録サーバと認証し，なりすましによる偽の登録を防止する．

2.3 システム構成

以上の機能を持つ GLI システムの構成図を**図 2** に示す．

- 登録クライアント
  移動体から GLI システムに対して，識別子と位置

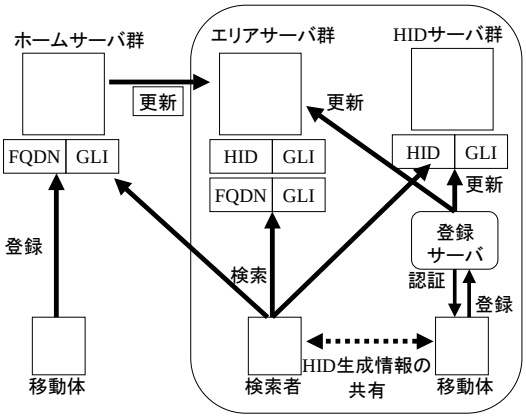


図 2 論理構成図
Fig. 2 Logical Architecture of the GLI System

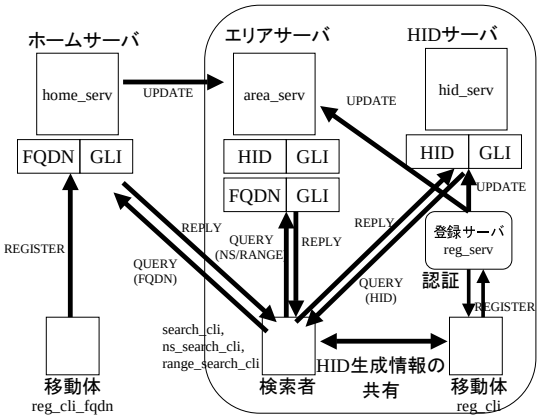


図 3 実装のシステム構成
Fig. 3 Architecture of the GLI System implementation

情報を登録する．オープンモードの場合は，FQDN と GLI をその移動体を管理するホームサーバに送信する．セキュアモードの場合，登録サーバに認証されてから，HID と GLI を登録サーバに送信する．

- 登録サーバ
  登録サーバは，セキュアモードの登録クライアントを認証し，HID と GLI の登録を受け付ける．HID と GLI を受信した登録サーバは，HID と GLI のそれぞれの値から HID サーバとエリアサーバを決定し，送信する．
- 検索クライアント
  検索クライアントは，サーバに対して検索要求を行うクライアントである．FQDN を用いた正引き検索の場合は，その FQDN から該当するホームサーバを決定し，検索要求を行い，結果を受信する．HID を用いた正引き検索の場合は，検索したい信頼関係にある移動体の HID を生成して，その HID から決定される HID サーバに対して検索要求を行い，結果を受信する．. 逆引き検索の場合は，検索の鍵となる位置情報から決定されるエリアサーバに対して検索要求を行い，結果を受信する．
- ホームサーバ/HID サーバ
  正引き検索を受け持つサーバである．ホームサーバと HID サーバは識別子の形式が異なるがサーバは区別しないためこれまで構築したホームサーバを HID サーバとして共用可能である．登録クライアントからの FQDN と GLI，および登録サーバからの HID と GLI を受け付けて登録する．
- エリアサーバ
  逆引き検索を受け持つサーバである．ホームサーバからの HID と GLI，および登録サーバからの HID と GLI を受け付けて登録する．

3. 実　　装

前章で述べたプライバシ保護機構を導入した GLI システムの実装を行う．移動体の識別子は FQDN と HID として，GLI(緯度・経度・高度) を登録し，ともに公開される．

3.1 モジュール構成

GLI システムは**図 3** に示すようなモジュールを実装して構成した，

プログラムは，FreeBSD4.5R において C 言語で実装されている，サーバ・クライアント間，サーバ・サーバ間の通信は，UDP を使用している．信頼性を向上させるため，確認応答とエコーバックさせ，RFC1323 の再送計算に基づいて再送させる機能 [8] を利用している．

登録クライアント

登録クライアントとして `reg_cli` および `reg_cli_fqdn` を実装した．`reg_cli` は，移動体にて動作し，HID を登録する場合に使用する．`reg_cli_fqdn` は FQDN で登録する場合に使用する．

登録サーバ

登録サーバとして `reg_serv` を実装した．`reg_serv` は，HID を使用して登録する移動体を認証し，その登録情報を HID サーバ，エリアサーバに転送する．

ホームサーバ/HID サーバ

ホームサーバおよび HID サーバとして，それぞれ `home_serv` と `hid_serv` を実装した．ホームサーバと HID サーバの機能は同じであり，識別子が HID でも

```
#ID          ts          ttl   r1    r2    r3
riho-m@sfc   969189102   600   123   456   789
icar1@sfc    969168349   300   345   678   321
```

図 4 **hid.conf** ファイルの形式
Fig. 4 format of **hid.conf** file

FQDN でも区別しないため，共用可能である．

エリアサーバ

エリアサーバとして area_serv を実装した．

検索クライアント

検索クライアントとして，search_cli, search_cli_fqdn, ns_serarch_cli， range_search_cli を実装した．それぞれ検索者において動作する．正引き検索は search_cli と search_cli_fqdn が行う．前者は HID を使用し，後者は FQDN を使用する．逆引き検索は，ns_serarch_cli, range_search_cli が行う．前者は最近接検索であり，後者は範囲検索である．

ライブラリ：GLILIB

登録クライアント，検索クライアントで使用される機能については，ライブラリを作成し，クライアントアプリケーションを開発を効率化している．本稿で実装した登録および検索クライアントもこのライブラリを使用しており，後述する．

HID 生成情報の設定

信頼関係にある移動体と検索者が共有する HID 生成情報は，あらかじめ共有されるが，本実装では hid.conf というファイルを持つことにより，共有する．信頼関係にある移動体と検索者とは，このファイルをオフラインかまたは安全な通信路にて交換するものとする．本ファイルは，HID での登録，検索時に使用される．

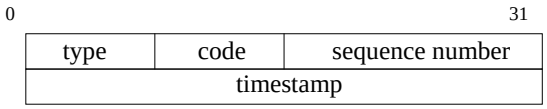
hid.conf の形式を，**図 4** に示す．

共有される HID 生成情報は，左から ID，timestamp，ttl，乱数値 3 個である．ID には形式のない任意の長さの文字列である．timestamp は基準時刻であり HID 生成情報を最初に作成した時刻である．単位は秒で，1970 年 1 月 1 日 00:00 を基準とした暦時間とする．ttl は HID 変更の間隔で，単位は秒．乱数値はそれぞれ 32bit の整数．

3.2 パケット構造

GLI システムのパケット構造は，ヘッダとデータに分れている．ヘッダでは，要求・応答の送信先・発信元を示す type と，処理内容を示す code，および再送計算用のシーケンス番号，発信時時刻がある．ヘッダの構造と type および code の内容を**図 5** に示す．

データ部では，登録・更新，および検索・応答時に送信される識別子，位置情報等がある．データ部は，type および code によって異なり，各処理の節で述べる．



type	code	
•REGISTER	•REQ_TO_RS	•REQ_TO_AS
•UPDATE	•REP_FROM_RS	•REP_FROM_AS
•DELETE	•REQ_TO_HS	•REQ_TO_HIDS
•QUERY	•REP_FROM_HS	•REP_FROM_HIDS

図 5 パケットヘッダ，および type，code の内容
Fig. 5 Packet header and values of type and code

3.3 登 録 処 理

移動体が識別子として FQDN を使用して登録を行う場合，reg_cli_fqdn は，GPS 等から取得された緯度・経度・高度と移動体の FQDN を，GLI_Reg_FQDN() に渡す．GLI_Reg_FQDN() は指定されたホームサーバに登録情報を送信する．

ホームサーバでは，登録クライアントから送信された登録情報を受信し，正引き検索用データベースに蓄積，管理し，登録する位置情報からエリアサーバを決定し登録情報を転送する．正引き検索用データベースは，Sleepy Cat 社によって公開されている Berkeley DB v3 を使用している．

エリアサーバでは，ホームサーバおよび登録サーバから送信された登録情報を受信し，逆引き検索用のデータベースで蓄積，管理する．逆引き用データベースには，SR-Tree[7] を使用している．

識別子として HID を使用する場合，HID を生成する必要がある．HID は設定ファイルに記述された設定情報を元に生成する．GPS 等から取得された緯度・経度・高度と移動体の HID 生成用 ID を，GLI_Reg_HID() に渡す．GLI_Reg_HID() は，ID から生成された HID，ID から md5 を使用して得られた MD，と位置情報を登録情報として登録サーバに送信する．登録サーバとは IPsec の ESP で通信を行い，はじめに認証を行ってから，登録情報の送信を行う．

登録サーバでは，登録クライアントから送信された登録情報から，転送すべき HID サーバ，エリアサーバを決定し，送信する．登録サーバは，登録クライア

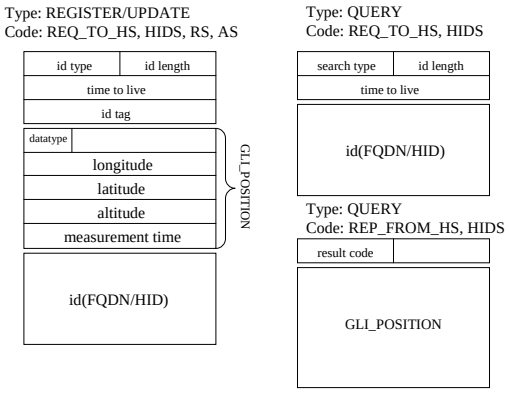


図 6 パケットデータ部 (1)
Fig. 6 Data part of Packet on GLI System(1)

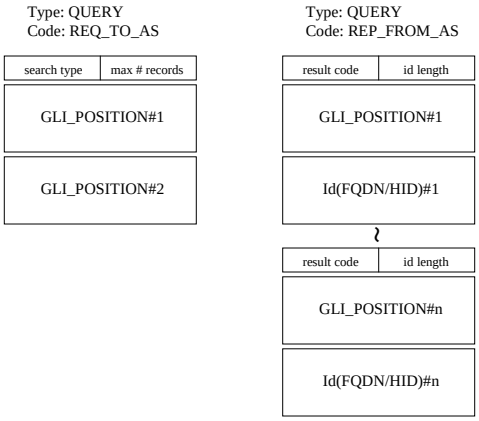


図 7 パケットデータ部 (2)
Fig. 7 Data part of Packet on GLI System(2)

ントからの MD と HID，転送先の HID サーバとエリアサーバのアドレスを管理している．HID が時間とともに変化するため，HID が変化した場合は，古い HID のレコードを消去するように，HID サーバ，エリアサーバに通知する．エリアサーバも登録する位置情報で決定されるが，転送先のエリアサーバが変化した場合には，古いレコードを持つエリアサーバに対して消去するように通知する．

登録に使用されるパケットのデータ部を**図 6** に示す．

3.4 正引き検索処理

FQDN を使用して正引き検索を行う場合，`search_cli_fqdn` では，指定された FQDN を `GLI_FQDNlookup()` に渡す．GLI_FQDNlookup() は，FQDN からホームサーバを決定し，検索要求を送信，結果を受信する．

HID を使用して正引き検索を行う場合，`search_cli` では，HID を生成するための ID を `GLI_HIDlookup()` に渡す．`GLI_HIDlookup()` は ID から HID を生成し，HID から HID サーバを決定し，検索要求を送信，結果を受信する．

正引き検索に使用されるパケットのデータ部を，図 6 に示す．

3.5 逆引き検索処理

`ns_search_cli` では，入力された 1 点緯度・経度・高度を `GLI_getneighbor_req()` に渡す．そこでは，渡された位置情報から検索要求を送信するエリアサーバを決定し，エリアサーバとソケットを開き，検索要求を送信する．`GLI_getneighbor_recv()` で結果を受信し，`GLI_getneighbor_close()` でソケットを閉じる．

`range_search_cli` でも，同様に入力された 2 点の緯度・経度・高度を `GLI_getrange_req()` に渡す．そこでは，渡された位置情報から検索要求を送信するエリアサーバを決定し，エリアサーバとソケットを開き，検索要求を送信する．`GLI_getrange_recv()` で，で結果を受信し，`GLI_getrange_close()` でソケットを閉じる．

エリアサーバでは，受信した検索要求により SR-Tree を検索し，検索結果を検索クライアントに送信する．

逆引き検索で使用されるパケットのデータ部を**図 7** に示す．

4. サンプルアプリケーションによる検証

実装された GLI システムのアプリケーションとして，タクシーのような配車管理を想定した最適車両決定アプリケーションを構築する．本アプリケーションの構築および実験を通じて，本システムの動作，有用性の検証を行う．

4.1 設　　計

本節で構築するアプリケーションでは，ある位置にいる客がタクシー会社の配車センタに迎車の要求を行ったときに，配車センターが客の周辺に存在する自社の車両から最適な車両を決定する手法を提供する．ここでは以下の事項を前提とする．

- 登録されている移動体は全て車両であるとする
- 他タクシー会社の車両も登録されており，識別はセキュアモードで行う
- 全て空車とする
- 配車決定は客の位置に最も早く到着できることを目指す

車両の決定の手順は以下のようになる．

(1) 客からの迎車要求が配車センタに→客の位置受信

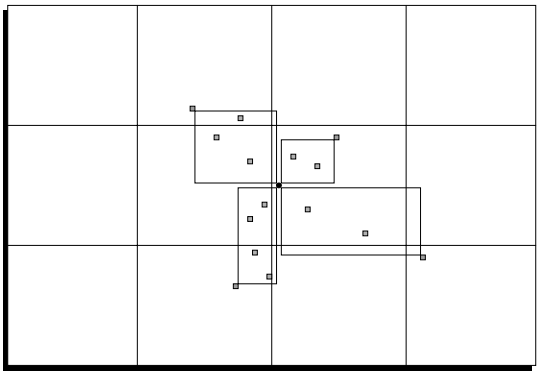


図 8 アプリケーション実行例
Fig. 8 example of result by application

(2) 客の位置から近い順に複数の自社の車両を検索する (逆引き:最近接検索)
(3) 客の位置から車両の位置までの範囲を検索する (逆引き:矩形範囲検索)
(4) 基準に従い，車両を決定する
(5) 車両に迎車の指令を送り，客の位置に向かわせる．

車両決定の基準としては，客とその周辺に存在するそれぞれの車両との距離とその間の混雑度を用いるとする．混雑度は，客の位置 A と車両の位置 B の 2 点間の距離 D と，2 点 A,B を含む矩形範囲の面積 S と，その範囲に存在する車両の台数 (N) の割合を基準として，次の式で表せると仮定する．

混雑度 $= D * N/S$

混雑度がより低い車両を決定する．

4.2 実 行 例

図 8 に本アプリケーションの実行例を示す．中央部の●が客の位置，周囲の■が車両を表す．客から車両までを範囲検索し，その範囲内に存在する第三者の車両を表示している．

5. まとめと今後の課題

本稿では，GLI システムを実装した．登録，検索の基本性能の十分な評価は間に合わなかったため，今後の課題としたい．より詳細な評価項目として，処理に要する時間の分析，登録されたレコード数と処理時間の関係，逆引き検索における範囲の広さと検索処理時間の関係などを挙げる．また，プローブ情報システム実験のデータを使用した実験アプリケーションの評価についても，今後評価することを課題とする．また，HID サーバ，エリアサーバの分散管理と，サーバの決定機能は今後実装してスケーラビリティ等の評価を行う．

謝辞

本研究において，評価用に IPCar の実験データを利用させて頂きました財団法人自動車走行電子技術協会様に感謝致します．本システムにおいてエリアサーバのデータベース機能として利用させて頂いている SR-Tree に関してご指導頂きました国立情報学研究所助教授片山紀生博士に感謝致します．また，貴重な御助言を頂いた WIDE プロジェクト，rover ワーキンググループ，インターネット自動車プロジェクト，慶應義塾大学環境情報学部村井研究室，政策・メディア研究科モービル広域ネットワークプロジェクトの皆様に感謝致します．

参 考 文 献

1) 和田光示, 特集:インターネットと自動車「プローブ情報サービス (IPCar) プロジェクト」, 情報処理学会誌 2002 年 4 月号, Vol.43, No.04
2) Yasuhito Watanabe, Atsushi Shionozaki, Fumio Teraoka, Jun Murai, “The design and implementation of the geographical location information system.”, Proc. of INET’96. Internet Society, June 1996.
3) Sohgo Takeuchi, Yasuhito Watanabe and Fumio Teraoka, ”The GLI System: A Global System Managing Geographical Location Information of Mobile Entities,” Trans. IEICE, Vol.E84-B, No.8, pp.2066-2075, AUGUST 2001.
4) 渡辺恭人, 竹内奏吾, 植原啓介, 寺岡文男, 村井純: プライバシ保護を考慮した地理位置情報システム, 情報処理学会論文誌マルチメディアネットワークシステム特集号, 42 巻 2 号, 2001
5) National Institute of Standards and Technology （NIST）, FIPS PUB 180-1: Secure Hash Standard, April 1995.
6) Krawczyk, H., Bellare, M. and R. Canetti, ”HMAC: Keyed-Hashing for Message Authentication”, RFC 2104, February 1997.
7) Norio Katayama, Shin’ichi Satoh, “The SR-tree: An Index Structure for High-Dimensional Nearest Neighbor Queries,” Proceedings of the 1997 ACM SIGMOD International Conference on Management of Data (May 1997) pp. 369-380.
8) W. Richard Stevens, 篠田陽一訳 “UNIX Network Programming Vol 1, 第 2 版, ネットワーク API: ソケットと XTI” ピアソン・エデュケーション, 1998