プライバシを考慮した地理位置情報システムの実装と評価

栗栖俊治[†1] 渡辺恭人[†2] 竹内奏吾[†3] 寺岡文男[†1]
[†1] 慶應義塾大学理工学部情報工学科 [†2] 慶應義塾大学 SFC 研究所
[†3] ソニーコンピュータサイエンス研究所

1 はじめに

インターネットと携帯端末の急速な普及により、地理的な位置情報を利用して移動するユーザの行動を支援するシステムやアプリケーションサービスが多く開発されており、地理位置情報を統一的に扱うシステムの構築が切望されている。インターネット上で移動体の地理位置情報を管理する機構として GLI(Geographical Location Information) システムが提案、実装されている [1]。GLI システムは全地球規模で移動体の地理位置情報を管理する大規模運用を目的としている。GLI システムはスケーラビリティを実現するためにサーバに階層構造を導入しているが、大規模な管理を行う上で、いくつかの問題がある。本論文では階層構造の実現手法の改良法を提案、実装し評価を行なう。

2 GLIシステムの概要

GLI システムは移動体の地理位置情報を地球規模で管理し、移動体の識別子を鍵とした地理位置情報の検索 (正引き検索)、地理位置の範囲を鍵とした移動体の識別子の集合の検索 (逆引き検索) をサポートする。また、移動体の位置情報に関するプライバシについても考慮がなされ、プライバシに関する問題の解決方法も提案されている [1]。

2.1 GLIシステムの構成

図 1 に GLI システムの構成を示す。GLI システムは位置情報を登録する移動体、これらの情報を管理する HID サーバとエリアサーバ、移動体の登録を受け付ける登録サーバ、及び検索者からなる。GLI システムでは地理位置情報に緯度経度を使用する。移動体の識別子には、移動体のプライバシを保護するために、移動体と、移動体と信頼関係にある検索者が共有する情報を鍵として、鍵付きハッシュ関数に作用させて生成した情報を用いる。以後、移動体の識別子を HID(Hashed ID) と呼ぶ (詳細は参考文献 [1] を参照)。HID サーバは正引き検索をサポートし、エリアサーバは逆引き検索をサポートする。また、HID サーバとエリアサーバは大規模運用を実現するために分散管理形態をとっている。登録サーバは、1 台で複数台の移動体を管理し、移動体と共通鍵を共有することで移動体を認証する。また、GLI システムにおいて、登録サーバは複数台存在するとする。

移動体は、GPS などの地理位置情報取得装置から最新の地理位置情報を取得する。移動体は登録サーバに自身の識別子と地理位置情報を登録する (図 1-(1))。登録サーバは、移動体の HID から決定される HID サーバに移動体の HID と地理位置情報を登録する。同時に、移動体の地理位置情報から決定されるエリアサーバに移動体の HID と地理位置情報を登録する (図 1-(2))。正引き検索を行う検索者は、移動体の識別子から決定される HID サーバに移動体の識別子を鍵として検索要求を送信する (図 1-(3))。検索要求を受信した HID サーバは、検索結果として地理位置情報を返す。逆引き検索を行う検索者は、地理位置の範囲を鍵とし、この領域から決定されるエリアサーバに検索要求を送信する (図 1-(4))。検索要求を受信したエリアサーバは、検索で指定された範囲内に存在する全ての移動体の識別子と地理位置情報を返す。

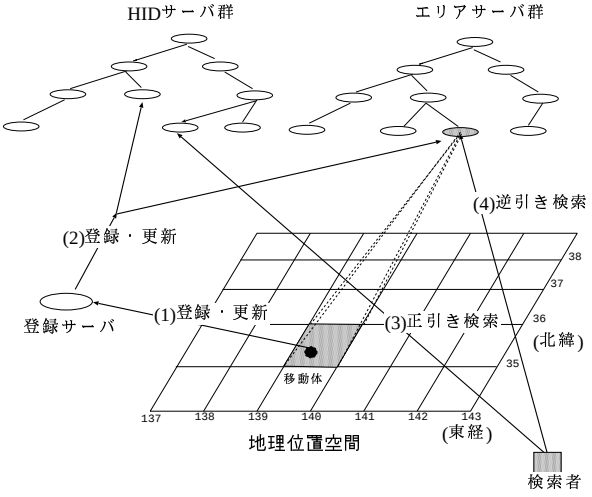

図 1: GLI システムの構成

2.2 GLIシステムの問題点

現在、HID サーバ群を分散管理するという方針はあるものの、HID サーバを分散化する手法の提案、実装がされていないという問題がある。また、エリアサーバは木構造による階層化手法をとっているが (参考文献 [2] 参照)、エリアサーバの管理領域が一意に示されないため、逆引き検索時に、逆引き検索クライアントからの委任情報要求が多数回にわたってエリアサーバに送信される問題がある。

本研究では上記の GLI システムの問題点を解決するために、HID サーバの分散管理の手法を提案し、実装する。同時に、エリアサーバの階層化手法の改良案を提案し、実装する。

3 HIDサーバの階層化

3.1 設計

HID は、移動体と、移動体と信頼関係のある検索者が共有する情報を鍵として HMAC-SHA1[3][4] に入力し生成した 160bit の数値である。本研究では、HID を数 bit ごとに区切って、区切った bit 列の値からその HID を管理する HID サーバを決定し、さらに階層化を行う手法を提案する。具体的には HID を 4bit ごとに区切って階層化を行い、その HID を管理する HID サーバを決定する。4bit ごとに区切ることで、160bit の HID に対し、最大 40 階層で任意の階層数が可能な階層構造を形成できる。4bit ごとに

区切ると、区切った bit 列の値は 16 通りとなるので、bit 列の値を 16 進数 (0 - f) に変換することで人間が理解し、運用もわかりやすくなるという利点がある。

図 2 に HID サーバの階層構造を示す。ルート HID サーバでは HID の先頭 4bit を 16 進数値 (0 - f) に変換し、その HID を委任する 1st Level の HID サーバを決定する。1st Level の HID サーバは、HID の先頭 5 - 8 bit 目を参照してその HID を委任する 2nd Level の HID サーバを決定する。同様に順次、各階層の HID サーバにおいて下位層に委任するサーバを決定すると図 2 に示すように最大 40 階層の階層構造を形成する。

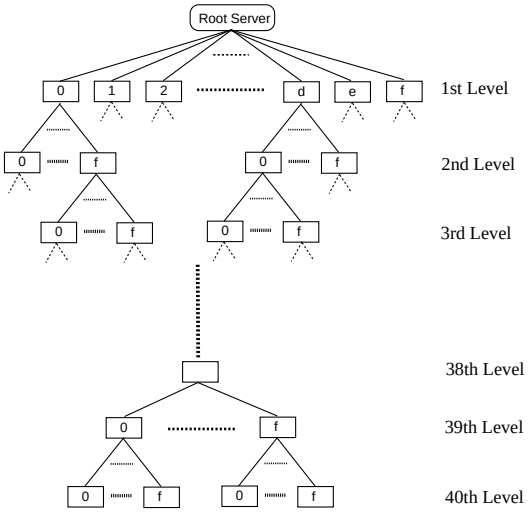

図 2: HID サーバの階層構造

3.2 登録時の動作例

図 3 に登録時の登録サーバと HID サーバ間の相互動作例を示す。以下に図 3 に示す環境において、HID:40515afb… d1f(図 3-(a)) の移動体の登録要求が発生してからの移動体、登録サーバ、HID サーバの動作を述べる。

1. 移動体は、移動体の HID と位置情報を含む登録要求を登録サーバへ送信する (図 3-(1))。
2. 登録サーバはルート HID サーバに移動体の HID を含むサーバ検索要求を送信する (図 3-(2))。
3. ルート HID サーバは、適切な 1st Level の HID サーバを決定する。次に、決定した HID サーバのアドレスと委任情報を登録サーバに返信する (図 3-(3))。
4. 登録サーバは、受信した委任情報をキャッシュし (図 3-(a-1))、委任情報で指定された HID サーバにサーバ検索要求を送信する (図 3-(4))。
5. HID サーバは、適切な下位層の HID サーバを決定する。次に、決定した HID サーバのアドレスと委任情報を登録サーバに返信する (図 3-(5),(7))。サーバ検索要求に含まれている HID が、サーバ検索要求を受信した HID サーバ自身が管理する値であった場合は、登録可能であることを登録サーバに通知する (図 3-(9))。
6. 登録サーバは、受信したデータが委任情報であった場合は、委任情報と階層構造をキャッシュし (図 3-(a-2),(a-3))、委任情報で指定された HID サーバにサーバ検索要求を送信する (図 3-(4),(6),(8))。受信したデータが、登録可能であることを示すデータであった場合、移動体の HID と位置情報をふくむ登録要求を送信する (図 3-(10))。
7. HID サーバは登録要求を受信すると、登録要求に含まれる移動体の HID と位置情報を登録し、登録確認応答を登録サーバに返信する (図 3-(11))。
8. 登録サーバは、HID サーバから登録確認を受信すると、移動体に登録確認応答を送信する (図 3-(12))。
9. 登録サーバは、新たに移動体から登録要求を受信するとキャッシュを参照し、適切な HID サーバへサーバ検索要求を送信する (図 3-(b) の場合は Server D)。

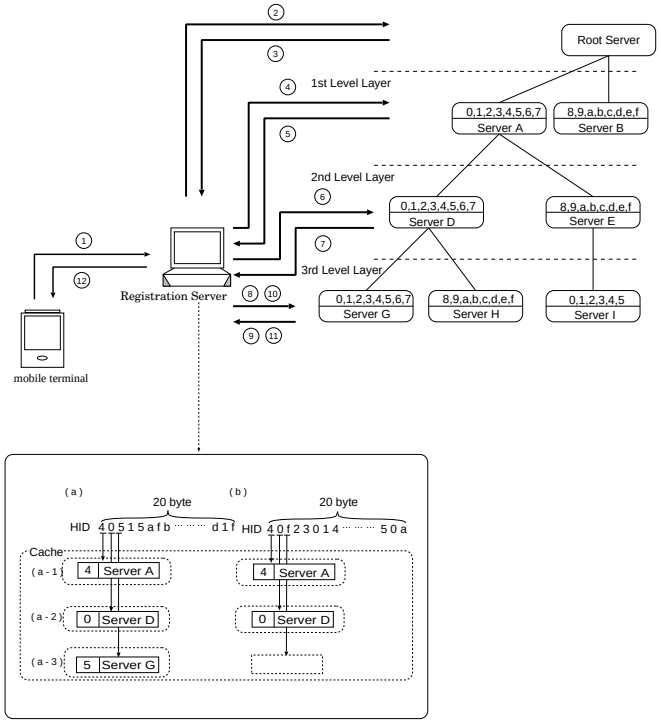

図 3: 登録時の登録サーバと HID サーバ間の相互動作例

4 エリアサーバの階層化

4.1 設計

既存の GLI システムのエリアサーバの階層化手法は、緯度経度の表記が度・分・秒で区切られていることを利用し、この区切りを一つのレベルとみなして階層化し、各階層において 1 度、1 分、1 秒四方の領域を管理するエリアサーバが存在すると仮定している。本研究では、各階層におけるエリアサーバごとに管理する領域の最低緯度、最高緯度、最低経度、最高経度を指定することで管理領域を決定する改良法を提案する。この改良法により、エリアサーバの管理領域が一意に示され、逆引き検索時の委任情報検索要求の発生回数を最低限にすることが可能となる。また検索クライアントでエリアサーバの管理領域をキャッシュすることが容易となる。

4.2 逆引き検索サーバの設置

本研究の分散管理の設計で運用すると、どの領域をどのエリアサーバが管理しているかという委任情報を検索するための通信が発生する。この検索をサーバ検索要求と呼ぶ。サーバ検索のたびにサーバ検索要求を送信すると、必ずルートサーバに問い合わせが到着することになる。また、ルートに近いサーバほどサーバ検索要求が多く到着し、サーバの負荷が高くなるという問題がある。この問題を避けるために、逆引き検索クライアント側でどのエリアサーバがどの領域を管理しているかという委任情報をキャッシュするようにするため、逆引き検索サーバを設置する。GLI システムにおいて逆引き検索サーバは複数台存在するものとする。

4.3 登録時の動作例

図 4 に登録時の登録サーバエリアサーバ間の相互動作例を示す。以下に図 4 に示す環境において、北緯 32 度 30 分 30 秒：東経 135 度 35 分 30 秒に存在する (図 4-(a)) 移動体 X の登録要求が発生してからの移動体、登録サーバ、エリアサーバの動作を述べる。

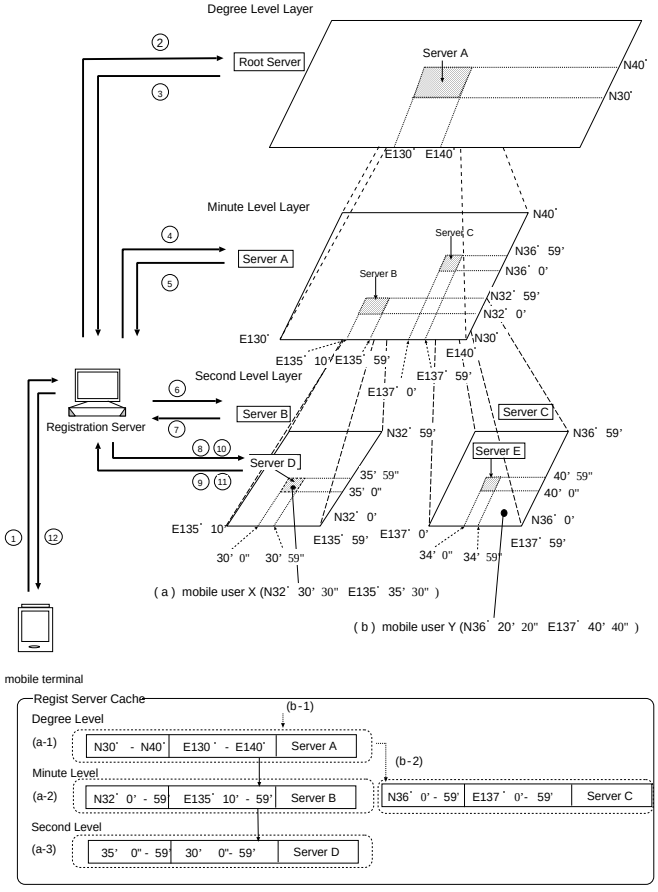

図 4: 登録時の登録サーバとエリアサーバ間の相互動作例

1. 移動体は、移動体の HID と位置情報を含む登録要求を登録サーバへ送信する (図 4-(1))。
2. 登録サーバは、ルートエリアサーバへ移動体の位置情報を含むサーバ検索要求を送信する (図 4-(2))
3. ルートエリアサーバは、サーバ検索要求に含まれる移動体の位置情報を参照し、移動体の存在するエリアを管理する Degree Level Layer のエリアサーバを決定する。次に、決定したエリアサーバのアドレスとそのエリアサーバの管理領域を含む委任情報を登録サーバに返信する (図 4-(3))
4. 登録サーバは、受信したデータが委任情報であった場合は、委任情報と階層構造をキャッシュし (図 4-(a-1),(a-2),(a-3))、委任情報で指定されたエリアサーバにサーバ検索要求を送信する (図 4-(4),(6),(8))。受信したデータが、登録可能応答であった場合、登録可能応答を登録サーバに返信したエリアサーバへ移動体の HID と位置情報を含む登録要求を送信する (図 4-(10))。
5. エリアサーバは、サーバ検索要求を受信するとルートエリアサーバと同様の処理を行う。登録要求を受信すると、登録要求に含まれる移動体の HID と位置情報を登録し、登録確認応答を登録サーバに返信する (図 4-(11))。
6. 登録サーバは、エリアサーバから登録確認を受信すると、移動体に登録確認応答を送信する (図 4-(12))。
7. 登録サーバは、新たに移動体から登録要求を受信すると (図 4-(b))、キャッシュを参照し、適切なサーバへサーバ検索要求を送信する (図 4-(b) では Server A)

4.4 検索時の動作例

図 5 に逆引き検索サーバとエリアサーバ間の相互動作例を示す。以下に逆引き検索要求が発生してからの逆引き検索クライアント、逆引き検索サーバ、エリアサーバの動作を述べる。

1. 逆引き検索クライアントは、検索領域の最低緯度、最高緯度、最低経度、最高経度を含む逆引き検索要求を逆引き検索サーバへ送信する (図 5-(1))。
2. 逆引き検索サーバは、逆引き検索要求で指定された検索領域をサーバ検索要求に格納し、サーバ検索要求をルートエリアサーバへ送信する (図 5-(2))。
3. ルートエリアサーバは、サーバ検索要求に含まれる検索領域を管理する下位層のエリアサーバのアドレスとそのエリアサーバの管理領域のリストを作成し、作成したリストを委任情報として逆引き検索サーバへ返信する (図 5-(3))。また、サーバ検索要求を受信したエリアサーバ自身が、サーバ検索要求に含まれる検索領域を管理している場合は検索可能応答を逆引き検索サーバへ通知する
4. 逆引き検索サーバは、委任情報をキャッシュし、委任情報にリストされている全てのエリアサーバへサーバ検索要求を送信する (図 5-(4),(8),(10),(14))。受信したデータが検索可能応答であった場合、検索可能応答を逆引き検索サーバへ返信したエリアサーバへ逆引き検索要求を送信する。(図 5-(12),(16))
5. エリアサーバは、逆引き検索要求を受信すると、逆引き検索要求で指定された検索領域内に存在する移動体の HID のリストを逆引き検索サーバへ送信する (図 5-(7),(13),(17))。

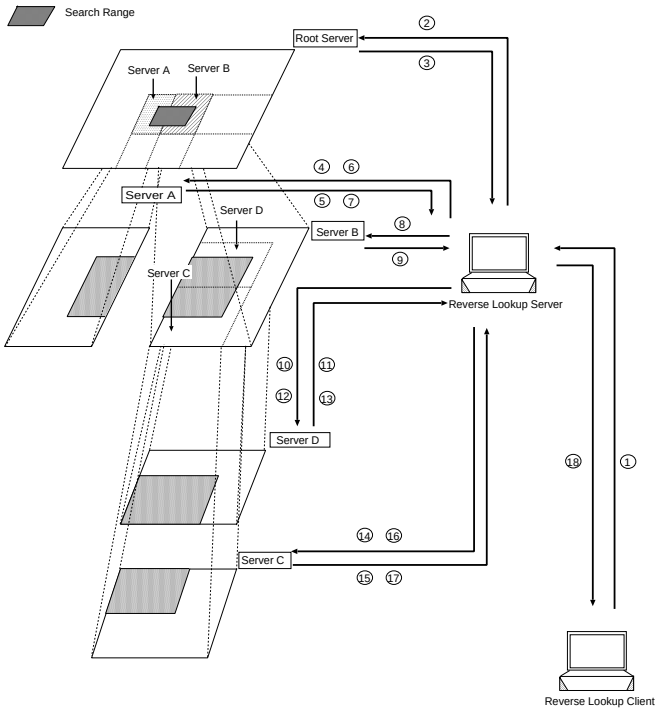

図 5: 逆引き検索とエリアサーバ間の相互動作例

6. 逆引き検索サーバは、逆引き検索要求を送信した全てのエリアサーバから HID のリストを受信すると、逆引き検索クライアントへ HID のリストを送信する (図 5-(18))。
7. 逆引き検索サーバは、新たに逆引き検索クライアントから逆引き検索要求を受信すると、キャッシュを参照し、適切なエリアサーバへとサーバ検索要求を送信する。

5 評価

HID サーバの階層構造を導入することにより増加すると思われるオーバヘッドを測定し、実装後の性能評価をする。オーバヘッドは、図 6 に示すように登録時の HID サーバにおける委任探索処理、および登録処理、そして登録サーバが HID サーバから委任情報を受信した際の、委任情報のキャッシュ処理がある。この 3 つについて測定を行い性能評価をする。測定は Intel 社製 Pentium4(1.7GHz)CPU 搭載の PC 互換機を使用して行った。

測定した結果を表 1 に示す。図 6-T1 は、HID サーバが登録サーバからサーバ検索要求を受信し、適切な HID サーバを探索・決定し、登録サーバへ委任情報を送信するまでの時間 (以後、委任探索処理時間と呼ぶ) である。図 6-T2 は登録サーバが、HID サーバから委任情報を受信し、委任情報をキャッシュしてから、委任情報に含まれる HID サーバへ登録要求を送信するまでの時間 (以後、キャッシュ作成処理時間と呼ぶ) である。図 6-T3 は、HID サーバが登録要求を受信してから、HID をデータベースに登録し、登録確認応答を送信するまでの時間である (以後、登録処理時間と呼ぶ)。なお、HID サーバのデータベースには db3 を使用している。

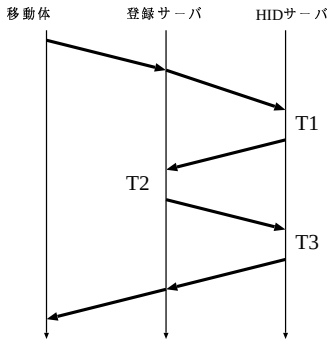

図 6: 登録時のメッセージフロー

HID サーバにおける処理では、委任探索処理時間が 0.243 ミリ秒、登録処理時間が 0.103 ミリ秒となっている。また、登録サーバにおけるキャッシュ処理時間も 1.07 ミリ秒となり、処理時間は短い。したがって、HID サーバが階層化されている環境では、登録にかかる時間の大部分を RTT が占めることがわかる。

表 1: 各サーバにおける処理時間

HID サーバにおける委任探索処理時間	0.243 ミリ秒
HID サーバにおける登録処理	0.103 ミリ秒
登録サーバにおけるキャッシュ作成処理	1.07 ミリ秒

6 おわりに

本論文では、移動体の地理位置情報管理システムである GLI システムの改良法を提案し、実装した。本提案方式では、HID サーバ群の分散化を実現し、さらに既存の GLI システムにおけるエリアサーバ階層構造の問題を解決した。また HID サーバの分散化によるオーバヘッドを測定し、性能評価をおこなった。今後はエリアサーバの分散化によるオーバヘッドの検討を行う予定である。

参考文献

[1] 渡辺恭人, 竹内奏吾, 寺岡文男, 植原啓介, and 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**, 42(2):234–242, February 2001.

[2] Sohgo Takeuchi, Yasuhito Watanabe, and Fumio Teraoka. The gli system: A global system managing geographical location information of mobile entities. *IEICE Transactions on Communication*, E84-B(8):2066–2075, August 2001.

[3] H Krawczyk, M Bellare, and R.Canetti. Hmac:keyed-hashing for message authentication. *RFC2104*, February 1997.

[4] P.Cheng and R.Glen. Test cases for hmac-md5 and hmac-sha-1. *RFC2202*, September 1997.