地理的位置情報の管理とアクセス制御に関する研究

和泉 順子　　砂原 秀樹
michi-i@is.aist-nara.ac.jp　suna@wide.ad.jp

奈良先端科学技術大学院大学 情報科学研究科
Graduate School of Information Science,
Nara Institute of Science and Technology

はじめに

- **急速なインターネットや携帯端末の普及**
- **モバイル・コンピューティングという計算機の利用方法**
- **インターネット上に固定または移動計算機が遍在**

  移動する計算機や、インターネットに接続できるエンティティの数は増大
  ⇒ その位置は広域に分散し、トポロジは常に変化

  計算機が移動するのに伴って、ネットワーク空間での位置の情報だけでなく現実空間での地理的な位置が必要になる場合がある

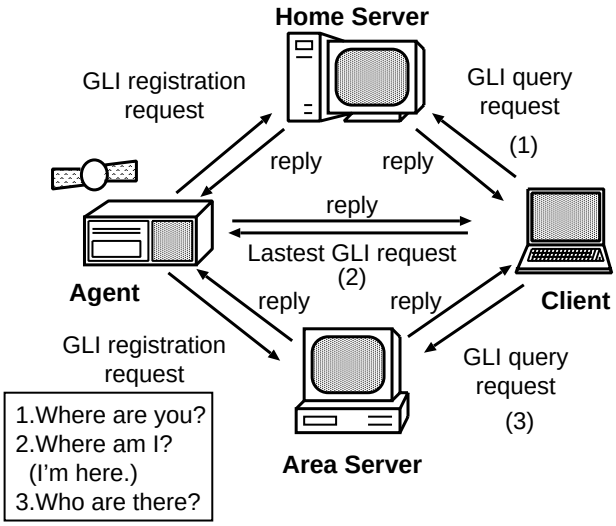
  ⇒ GLI(Geographical Location Information)**システムの構築**

GLI(Geographical Location Information)System

GLI System

移動する計算機の地理的な位置情報と、ネットワーク中のエンティティとの対応を管理する機構

WIDE InternetCar Project **で実際に用いられている**



GLI(Geographical Location Information)System ($cnt'd$)

問題点 (セキュリティ機能の欠落)

不特定多数の無制限な利用 $\Rightarrow$ 利用者のプライバシや行動を侵害

問題解決には…

- **公開してもよい地理的位置情報（GLI データ）と そうでないもの（情報の所有者など）との区別が必要**
  GLI **データ：緯度, 経度, 高度, ベクトル (速度と方向), 時刻**
- GLI **データ管理するための** ID **に関する工夫が必要**
  （そのまま 個人を識別できるような ID **では意味がない）**

研究目的

セキュリティ（プライバシ保護）を考慮した地理的位置情報管理システムの提案とプロトタイプの設計

1. GLI システムの構成要素へのアクセス制御機能の付加
   (公開情報と非公開情報の区別)

   ⇒ 共通鍵暗号を用いたデータの暗号化と、そのデータに対する ACL(Access Control List) の付加

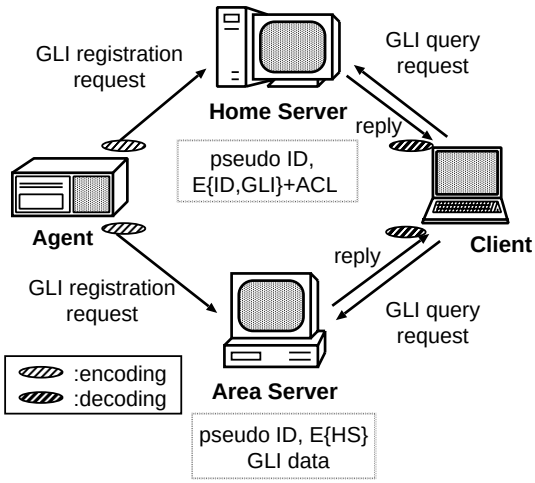
2. 情報管理のための ID と情報自体との直接のつながりをなくす

   一方向性ハッシュ関数（または 暗号化？）を用いた pseudo ID の生成の検討

提案する設計モデルの概要

- 暗号化した情報をサーバに蓄積／管理するアーキテクチャの設計モデル
- それだけでは個人を識別できないような ID (pseudo ID) の考察

情報管理の権利がある程度情報提供者にあると考えられ、復号鍵を持つ者だけが意味のある情報を取得可能



現状-情報の暗号化-

地理的位置情報データの暗号化

⇒ **共通鍵暗号**
OpenSSL 0.9.4 **暗号化ライブラリの** tripleDES CBC mode **の関数**
EVP_des_ede3_cbc() **を用いている**

アクセス制御

⇒ **暗号化した地理的位置情報データに** ACL **を付加する**

鍵配送問題

共通鍵暗号で用いた鍵の配付や認証に、公開鍵暗号または KPS(Key Predistribution System) **などの仕組みが必要**

現状 -ID と pseudo ID-

ID（GLI 情報を管理するためのネットワーク上の識別子）

現在の GLI **システムで用いられている ネットワーク空間の識別子**

- IP **アドレス**
- FQDN(Fully Qualified Domain Name)

⇒ **この識別子を見ただけで その情報を送信した計算機が分かってしまう**

このシステムで重要な挙動は

- ID **は固定ではない（**ID **を検索しただけで身元が分かるようでは意味がない）**
- **必要な情報は適宜、権限を持つ者によって 引き出せる**
- **閉じたアプリケーションの中でのみ 意味のあるデータを保存**

⇒ pseudo ID **の導入**

現状 -ID と pseudo ID- $(cnt'd)$

pseudo ID の必要条件

- real ID との binding は HS で管理
- real ID や他の情報から類推されない
- Agent で生成され、各サーバに登録される
- Client が生成する可能性もある

ここで、

1. pseudo ID の計算にハッシュ関数を用いる場合、悪くとも共通鍵暗号と同程度の速度がなければ実用的価値に乏しい

   汎用一方向性を満たすハッシュ関数 : SHA-1, MD5 など
   鍵付ハッシュ関数についても調査中

2. pseudo ID の計算を暗号化で行なうのであれば、その鍵配送に問題が残る (GLI データと同じ鍵で暗号化するか？)

提案手法の実用性の検証

現在考えている pseudo ID 導入を含めたモデルを検討後、アーキテクチャを設計し、プロトタイプとして実装する

そのプロトタイプシステムが、セキュリティ機能を付加した GLI システムとして、機密性、完全性、認証を保つことができること検証する

その上で、本研究のプロトタイプと Original GLI システムとの性能比較を行い、実用的価値の検証を行う

まとめ

セキュリティ面を考慮した、地理的位置情報管理システムに対するアーキテクチャ設計のためのモデルを提案した
また、情報のプライバシ保護のため、pseudo ID を導入することを検討した

今後の課題

- **共通鍵を共有する人の決め方と鍵の配付方法**
- pseudo ID **の 有効期限について**
  e.g) **登録毎に変える、一定の登録回数毎に変える…**
- **広域分散環境での振舞いについて**
- **通信の秘匿性 (通信の事実を隠すこと) の問題**

Appendix

GLI システムに関する文献

- The Design and Implementation of the Geographical Location Information System
  Yasuhito Watanabe, Atsushi Shinozaki, Fumio Teraoka, Jun Murai
  Proc INET'96
- インターネットを利用したモバイルユーザの地理位置検出システムの構築
  竹内 奏吾
  電気通信大学大学院 情報システム学研究科（修士論文）

KPS に関する文献

- 暗号鍵を通信なしで共有する方法：Key Predistribution System
  松本 勉 今井 秀樹
  電子情報通信学会論文誌 A Vol.J71-A No.11 pp.2046-2053 (Nov.1988)
- The ID-based Key Management System(IDKMS)
  draft-rfced-info-kubo-00.txt
  INTERNET DRAFT Expires Jan 1999

Appendix ($cnt'd$)

鍵付ハッシュ関数に関する文献

- HMAC: Keyed-Hashing for Message Authentication
  rfc2104 (February 1997)