修士論文：2006 年 3 月修了

位置情報プライバシーに関する研究

-A Research on Location Privacy-

環境学専攻　社会文環境コース
46843　山根　弘
指導教員：瀬崎薫助教授

キーワード：位置情報,プライバシー,無線通信,RFID,匿名性

１．研究の背景

ユビキタス情報環境において人あるいはモノの位置情報は非常に重要である．位置情報は個人のコンテキスト（ユーザの置かれている状況）を判断する大きな要素となり，コンピュータがそのようなユーザのコンテキストを判断することで，コンピュータが自発的にサービスを提供していくことができるためである．特にユーザの位置に応じたサービスは位置情報サービス（LBS : Location Based Service）と総称され，これらのサービスを実現するための種々の測位技術が開発されてきている．

このような測位技術はユビキタス情報環境においては不可欠である一方，個人の位置情報プライバシーを侵害する危険性もある．本論文においては位置情報プライバシーの侵害を「特定の個人が長時間にわたり第三者に追跡されること」と定義している．ユビキタス情報環境において我々の位置情報プライバシーが侵害される問題を指摘するとともに，その解決手法を提案している．

２．想定環境および攻撃者モデル

我々はまず無線 LAN や Bluetooth といった無線通信端末を使用するユーザの位置情報プライバシーの問題に着目した．個人がこれらの端末を利用する際,個人の意図とは関係なく第三者が個人の位置情報を取得することができる環境にあり,その位置推定精度は数 m にまで向上してきている.このような問題に対して位置情報の識別子にあたる MAC アドレスを更新することで追跡を回避しようといったことが既に提案されている[1]．しかしながら高精度・高頻度の測位環境においては仮に識別子を更新したとしても，それらの位置情報の相関を利用して位置情報を関連付け，さらに追跡されてしまう危険性がある．本研究においては位置情報の相関の中でも特に時間的・空間的相関を利用した追跡を行う攻撃者モデルを定めた．このような中では位置情報プライバシー保護のためには識別子を変更するだけでなく，新しい識別子の匿名性を十分に保障するための手法を考えていく必要がある．

３．Silent period の提案

我々は前節で述べた目的に従って”silent period”と呼ばれる手法を提案している．アドレス更新の間に，いっさい通信を行わない期間を設けることにより，更新前後のアドレスが測位される位置情報の相関を小さ

くする効果が期待される．このことにより，更新前後のアドレスが同一のユーザに属していると推測することが困難となると考えられる．図１にはユーザ２人に対して silent period プロトコルの一例を示している．ユーザ１とユーザ２が同時に silent period にはいり，それぞれアドレスを A→A’，B→B’に更新している．ユーザ１を追跡しようとしている第三者の立場からみれば，A’，B’ともにユーザ１の新しいアドレスの候補となるため，ユーザ１の本当のアドレス A’は，その匿名性が確保されているといえる

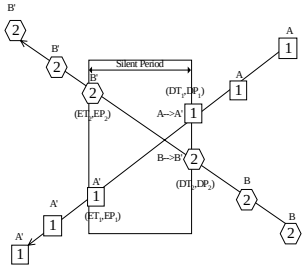

図１: Silent period

さらに位置情報プライバシーといった概念的なものを定量的に評価するために匿名通信におけるアノニミティセット[2]を応用し，GAS(Geographical Anonymity Set)と呼ばれる概念を提唱した．GAS とは特定の位置情報と時間的・空間的に相関のある位置情報の集合であり，GAS のサイズあるいはエントロピーといった数値指標がプライバシーの定量的解析・評価に有効である．

図 2 には GAS を用いた silent period の評価結果を示す．特定のエリア内で移動するユーザの位置情報プライバシーをシミュレーション評価したものである．これをみると silent period が長いほど GAS のサイズが大きくなっていることがわかる．つまりある位置情報に対してそれと時間的・空間的に相関のある他の位置情報が多くなり，攻撃者にとってみれば特定の個人を追跡しにくい環境が生まれていることがわかる．長い silent period により個人の位置情報プライバシーのレベルは向上するといえる．

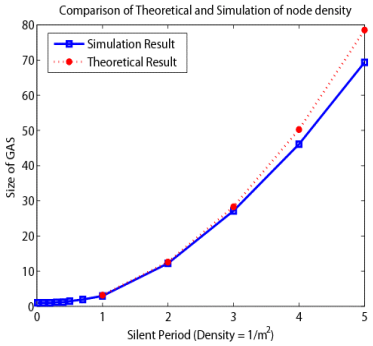

図２:GAS に基づく評価

４．QoS の考慮

長い silent period を設けることにより，プライバシーレベルが向上すると考えられるが長い silent period はサービス品質（QoS）に大きな影響を及ぼす．例えばストリーミングなどのリアルタイムアプリケーションの場合，無線パケットは連続的にブロードキャストされる環境にありデータの遅延は QoS の劣化を招く．また HTTP あるいは FTP などのノンリアルタイムアプリケーションの場合でも，silent period が長いとユーザが欲する時にアプリケーションを使用できない事態が起こる．

以上のように QoS の制約を考慮すると，プライバシー保護の一点のみに着目し,むやみに長い silent period を設けることは不適切であることがわかる．そこで我々はプライバシーレベルと QoS レベルの両立を実現するために,従来の匿名通信で議論されていた Mix-cascade の手法を位置情報プライバシー保護に応用し，多段的に silent

period に入ることによりプライバシーを保障するといったプロトコルを提案する．これを silent cascade と呼び,図 3 にその概要を示す.個々の silent period の値は QoS の制約を満たしつつも，小さなプライバシーレベルの向上に貢献する．ただ，そのような個々の silent period を多段的に繰り返すことで，結果として十分なプライバシーレベルが保障されることとなる．なお，本システムにおいて同一のアドレスを使い続ける期間を Address lifetime と定義している．システムを設計する際には silent period の長さと address lifetime の長さを適切に設定する必要がある．

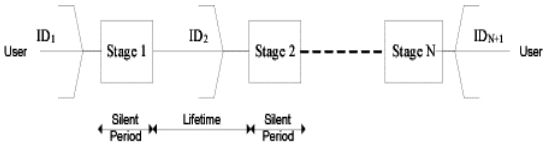

図 3 : Silent cascade

Silent cascade におけるプライバシーレベルと QoS の関係を考察するためにシミュレーション解析を行った．プライバシーレベルの指標としては攻撃者が追跡できる時間を直接指標とした追跡時間(MTT)を利用した．また QoS のメトリックとして通信不可能な時間の比率を示す CLR を定義した．これは silent period と lifetime の比で与えられるものとする．このような指標に基づいて，一定の QoS レベルの中で最大のプライバシーレベルを実現するような silent cascade のパラメータの値を検証した. 図 4 においては，QoS の指標である CLR を固定した中での，lifetime と追跡時間との関係についてシミュレーションから得られたグラフを示している．このグラフをみると，追跡時間を最小とする最適な lifetime が存在していることがわかる．より詳細にこの最適な lifetime の値をみるために，我々は幾何学的な計算に基づく MTT と lifetime の関係の定式化をおこなった．CLR を c, lifetime を L，ノード密度を D, 速度を v とし, MTT を L の関数として書くと以下のようになる．

$$MTT(L) = \frac{a}{L} + \frac{L}{2} \quad where \quad a = \frac{1}{D \cdot \pi \cdot (c \cdot v)^2}$$

極小値を与える L は $L = \sqrt{\frac{2}{\pi D c^2 v^2}}$ となる．

一定の QoS レベルを前提とした中で，最小の追跡時間，つまり最高のプライバシーレベルを実現するこの address lifetime の値は，最適な lifetime ということができる．また，最適な lifetime の値にノード密度 D といったパラメータが含まれていることから，最適な lifetime はユーザが属する環境のノード密度に依存するといえる.実世界での利用を考えるとユーザの属するノード密度は時々刻々と変化するものであるため実際に silent cascade を設計する際には環境に合わせて lifetime の値を動的に制御していく機構が必要とされると考える．

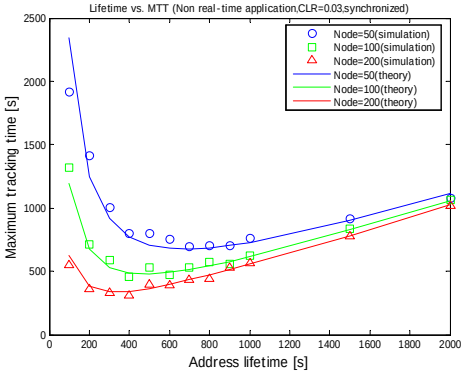

図 4: 最適な address lifetime

５．RFID への応用

Silent period は無線通信端末の分野のみに限った位置情報プライバシー保護手法ではない．基本的に識別子 *id* を変えて追跡を回避しようとする中で識別子変更前後の位置情報の非結合性を高める手法であり，幅広い分野で応用可能な手法である考えている．我々はこの silent period の手法を RFID システムにおける位置情報プライバシー保護に応用することを考えた．

RFID(Radio Frequency Identification)は無線を利用した自動認識システムであり，バーコードに変わる商品識別手法として注目されている．あらゆる商品にタグを取り付け，流通の効率化が図るといった EPC プロジェクトなど様々な使用用途が提案されているがセキュリティの面で不安を残している．その一つとして位置情報プライバシーの問題がある．RFID のシステムにおいてはタグはリーダーの問い合わせに対して自身の ID を応答するのだが，この ID が測位される位置を第三者が取得することで，特定の個人が追跡されることが危惧されている．このような追跡問題を回避するためには応答する ID を固定ではなく可変とし，かつ各 ID で測位される位置情報の非結合性を高める必要がある．我々はこの部分に silent period を適用することを考えた．無線通信端末の場合と RFID の場合では測位形式，得られる位置情報の形式，そして ID 更新の同期制御といった異なる点がある．特に ID の更新が各タグで非同期に行われることは，時間的に相関をもつ位置情報の減少につながり，攻撃者が追跡しやすい環境をつくる．我々はこのような点に考慮した結果，silent period の長さを可変長にすることを提案した．図 5 にはその評価結果を示す．Silent period における可変部分の割合(variable ratio)をより大きくした場合により高いプライバシーレベルが実現されている．これは可変長の silent period により時間的に相関をもつ位置情報の集合が大きくなったためだと考えられる．

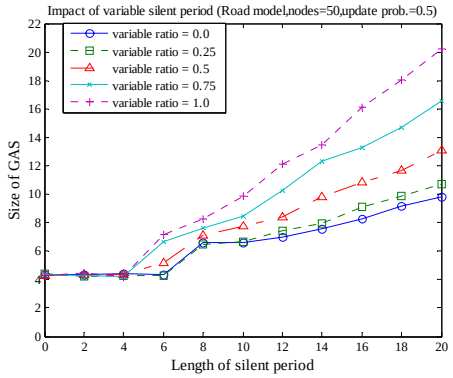

図 5：RFID における評価

６．結論

本研究においては時間的・空間的相関を利用した追跡問題を指摘するとともに，その解決手法として silent period の手法を提案した．また評価手法として GAS といった概念を提案し，silent period の有効性を示した．さらにプライバシーと QoS の関係について考察し，一定の QoS 制約の中でもより効率的にプライバシー保護できるシステムの設計指針を得た．最後に本手法が RFID といった他分野にも応用可能であることを示した．

文　献

[1] M. Gruteser, "Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis," 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots, 2003.

[2] L. Sweeney. :k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 2002