

東京大学大学院新領域創成科学研究科
環境学専攻社会文化環境コース

平成 17 年度

修士論文

位置情報プライバシーに関する研究

2006 年 1 月 31 日提出
指導教員 瀬崎 薫 助教授

46843 山根 弘

目次

1	序論	1
2	研究の背景	3
2.1	ユビキタスコンピューティングと測位技術	3
2.2	プライバシー侵害の脅威	5
2.3	先行研究	6
3	無線通信端末における位置情報プライバシー	10
3.1	想定環境	10
3.2	攻撃者モデル	11
3.3	追跡アルゴリズム	14
4	Silent period の提案	18
4.1	Silent period	18
4.2	評価手法の検討	19
4.3	評価	22
5	Silent cascade の提案	26
5.1	QoS とプライバシー	26
5.2	Silent cascade の提案	27
5.3	評価	31
5.4	考察	35
6	RFID への応用	38
6.1	背景	38
6.2	想定環境	41
6.3	RFID におけるプライバシー保護手法	44
6.4	評価	46
7	結論	51

1 序論

本論文においてはユビキタス情報環境における個人の位置情報プライバシーの問題を取り扱っている. ユビキタス情報環境においては人あるいはモノの位置情報といったものが非常に重要視され, 多くの位置取得技術が研究・開発されてきている. それらの位置推定精度は向上し, また屋内・屋外問わずにあらゆる場所で個人の位置情報を取得できる環境が整いつつある.

このような位置情報は非常に有用である一方, 位置情報が不当に第三者に取得される場合, 個人のプライバシーが侵害されることが懸念される. 個人がいつ, どこにいたのかといった情報もちろん, 場合によっては何をしていたのかといった行動までが第三者に推測される危険性もある. 場所とその場で行われる行動といったものの間には密接な関係がある場合が多々あるためである.

本研究における位置情報プライバシー侵害の定義は「特定の個人が第三者によって長時間に渡り追跡されること」としている. 長時間にわたり追跡されることはより多くの行動を推測されるといったことだけではなく, 位置情報の匿名性の確保の大きな影響を与える. 一般的にユビキタス情報環境で測位される位置情報の識別子とは個人の实名であることは少なく, 個人の所有するモノの識別子(無線通信端末のアドレス)などである場合がほとんどである. 位置情報の識別子がこのようなモノの識別子である限りにおいては個人のプライバシーに直接的な影響はないと考えられるが, 長時間に渡り追跡されることで, 第三者がモノの識別子から個人の实名までも推測する場合がある. このような場合, 位置情報の匿名性が失われ, 個人のプライバシーが侵害されると考えられるため, 特定の個人が長時間に渡って追跡されないようにすることはプライバシー保護において重要な意味をもつ.

我々は個人が追跡されるおそれのある環境の中でも, まず無線通信端末の利用に着目し, それを使う個人の位置情報プライバシー保護手法を検討した. またプライバシー保護といった一面からの分析ではなく, プライバシーと無線通信端末を利用したアプリケーションの品質との関係にも着目し議論を進めた. ユビキタス情報環境における利便性と安全性, その両立を図ることが目的である. そしてさらにこの分野で提案した手法を他分野にも利用することを考え, **RFID** システムにおける位置情報プライバシー保護に関して検討を行った.

本論文の構成は以下の通りである. まず2章において研究の背景として, ユビキタス情報環境における位置情報およびその取得方法について概要を述べた後, 位置情報プライバシー侵害の問題を提起し, またプライバシーに関する先行研究を紹介す

る.3 章において本論文でまず着目した無線通信端末の分野に関して,その想定環境を整理する.また個人の位置情報プライバシーを侵害する攻撃者モデルとして時間的・空間的相関を用いた追跡といった攻撃手法の存在を指摘するとともに,具体的な追跡アルゴリズムに関して検討を行う.ここで述べたような想定環境において攻撃者からの追跡を回避し位置情報プライバシーを保護する手法として4 章において”silent period”と呼ぶ手法を提案する.また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の手法を考察し,その手法に基づき評価・解析を行う.5 章においては個人のプライバシーといった安全性と個人の使用するサービスの品質といった利便性の両立を図るための手法として silent period から Silent cascade といった手法に拡張し,その評価・解析を行っている.そして6 章においては本手法を無線通信端末以外の分野にも応用していくことを考える.本研究においてはその分野の一つとして RFID システムにおける位置情報プライバシーの問題に着目し,その環境を整理するとともに本手法を適用し,その有効性を示している.最後に7 章において本論文の結論および今後の課題を述べる.

2 研究の背景

2.1 ユビキタスコンピューティングと測位技術

コンピュータの利用形態は時代とともに大きく変化してきている。従来は複数の人で一台のコンピュータ（メインフレーム）を使用していたのだが、最近では1人で1台のコンピュータ（パーソナルコンピュータ）を使うことは一般的なこととなっている。そして、これらに続く第三世代のコンピュータ利用形態として「ユビキタスコンピュータ」といった概念がいられている。これは1991年にアメリカのマーク・ワイザーによって提唱された概念である[1]。ユビキタスとはラテン語の「偏在する」「いたるところに存在する」という意味の語を語源としており、ユビキタスコンピューティングとは実世界のあらゆる場所にコンピュータが存在しており、それらにアクセスできるような環境を示している。アクセスに使う端末は一般的なパソコンや携帯電話だけに限らず、家電製品や自動車などもネットワークに接続されつつあり、またウェアラブルコンピュータと呼ばれる身に付けるコンピュータも開発されている。

従来の利用形態と異なり1人で複数のコンピュータを利用するようになると、多すぎるコンピュータの存在に煩わしさが生まれるかもしれない。このような状況にならないようにワイザーはコンピュータが「見えない(invisible)」ことを強調している。このために人間とコンピュータとのインターフェースに関しても従来のようなキーボードとマウスに依存する入力形態ではなく、コンピュータがユーザあるいはその置かれている環境の”状況”を判断し自発的にサービスを提供していくような動作形態が目標とされている。この判断の基準となるユーザ・環境の状況をコンテキスト(context)と呼び、文献[2]においては以下のように定義されている。

Context is any information that can be used to characterize the situation of an entity.

このようなユーザのコンテキストを判断し、ユーザにサービスを提供していくことはコンテキストウェアサービスと呼ばれる。上記の定義に表現されるようにコンテキストには種々の情報が含まれるが、実世界でのコンピュータの利用を考えたい際にもっとも重要なコンテキストがユーザあるいはモノの位置情報であるといわれる。ここで位置情報とは識別子 id 、空間 s 、時間 t から構成される情報とされる。コンテキストウェアサービスの中でも特にユーザの位置に応じたサービスを行うものは位置情報サービス(LBS:Location Based Service)と呼ばれ、既に実用化され

ているものも多数存在する．たとえば移動する車の位置情報を取得して目的地までの経路を提示するカーナビゲーションシステムなどは既に広く普及しているし、近年では携帯電話に位置取得機能をもたせることで、車に限らず移動するユーザに対してナビゲーションを行うサービスも登場してきている [8]．

ユビキタス情報環境において重要な位置情報を取得するために様々なデバイス・手法による位置取得術が研究・開発されてきている．現在、利用可能な測位技術の多くは、測位方式によって三点測量方式と近接検知方式との2つに分類される．代表的な測位デバイスの例を図1に示す．

三点測量方式とは複数の位置のわかっている何らかの基地局から測位対象までの距離を測定し、その距離情報をもとに三点測量の原理で測位対象の位置を推定する方式である．距離の測定には電波を利用することが多い．基準位置から測位対象までの電波の到達時間を利用した TOA(Time of Arrival)/TDOA(Time Difference of Arrival) 方式、あるいはその区間での電界強度の損失量を利用した RSSI(Received Signal Strength Indicator) 方式などが一般的である．この方式に基づく測位デバイスとしては GPS (Global Positioning System) , 無線 LAN そして超音波などがある．GPS の場合には基地局として米国国防総省により管理される人工衛星が使われ、距離推定は TDOA 方式に基づいている．従来は米国の安全保護の名目のもと測位精度が意図的に制限され、測位誤差が 50m から 100m 程度であったが、2000 年 5 月にはこの制限が解放され精度が 5m から 10m 程度にまで向上した．さらに地上にも基地局を配置し、測位結果の補正を行う D-GPS(Differential GPS) といった手法などにより、なお精度が向上してきており、主に屋外での測位に多用されている [11]．無線 LAN での測位の場合は基地局として無線 LAN のアクセスポイントなどが使用され、ユーザの所有する無線 LAN 端末の発する電波を用いて TOA/TDOA 方式あるいは RSSI 方式に基づいて測位される．日立製作所の開発した Air Location といったシステムでは TDOA 方式を用いることで誤差数 m での測位が実現されている [4]．また超音波センサの場合は音波の到達時間差を用いて距離推測を行うものであり、より低コストのデバイスで測位環境を構築することができる [10]．これらは主に GPS が機能しない屋内での測位のために用いられることが多い．

一方、近接検知方式とは位置の分かっている何らかの基地局に測位対象が近づいたことを検知し、その基地局付近に存在しているといった情報を取得する方式である．この方式に基づく測位デバイスとしては赤外線、磁気コイルセンサ、そして RFID などが代表的である．赤外線の受信機を環境中に配置し、ユーザの所有する赤外線送信機の信号を受信することで測位する Active badge[12] は屋内での測位デ

バイスの先駆者的な研究であった。また2つのコイルの相互誘導を利用した近接検知として磁気コイルセンサでの測位も試みられている [9]。RFID に関しては国土交通省が中心となり、道路などに IC タグを埋め込み、都市環境全域において近接検知方式の測位を可能とするスケールの大きなプロジェクトも進められている [14]。

またこの他にもカメラを利用した画像認識による測位方式や、ウェアラブルセンサ（加速度センサなど）を利用した慣性航法方式などの測位デバイスも開発されている。これらの多くの測位デバイスを組み合わせて使用することでいつでもどこでも測位可能な環境が実現されつつある。

Triangulation



Proximity detection

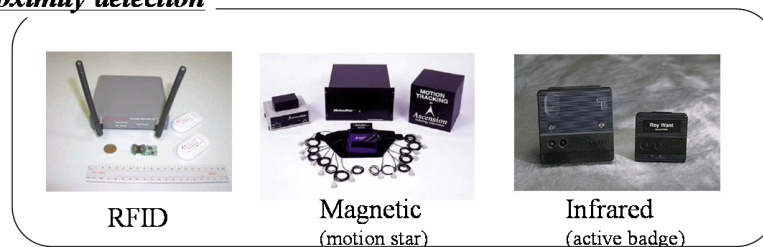


図 1: Positioning devices in ubiquitous computing

2.2 プライバシー侵害の脅威

多くの国において人の基本的な権利としてプライバシーを守る権利を定めている。国内においても 2005 年 4 月からは個人情報保護法 [38] が全面的に施行され、プライバシーの関心は年々高まってきているといわれる。前節で述べたような多くの位置情報取得技術は、ユビキタス情報環境において多くの有用なサービスを実現してくれる一方で、位置情報プライバシーを侵害し得ることが懸念されている。

ユーザの訪れる先々で位置情報 (is, s, t) が第三者に取得されることはユーザのプライバシーに多大な影響を与えると考えられる。まず位置情報といったものには必

ず何らかの識別子 *id* 情報が含まれている. そのため個々の位置情報を取得可能な第三者は, 同一の識別子の位置情報を結合することで, 特定のユーザの長時間にわたる移動履歴を取得することが可能となる. また移動履歴が知られるということは, ユーザが知られたくない別の情報まで知られる可能性がある [32]. たとえばあるユーザが病院にいったということが分かった場合, 第三者はそのユーザは病気であるかもしれないといった情報を推測をすることができる. このような秘密にしておきたいようなプライベートな情報まで侵害されることは大きな問題であるといえる.

ただしここで注意しておかねばならないのは識別子 *id* の扱いである. この *id* は測位デバイスによって異なるが, たとえば GPS 内蔵の携帯電話で測位する場合は携帯電話の番号・アドレスなどが *id* となるであろうし, 無線 LAN の場合であれば, その端末に割り当てられた MAC アドレスが位置情報の *id* となる. 特殊な場合をのぞいて, 第三者の立場からみれば, その識別子からその端末を所有する人の実名・本名を割り出すことは難しい場合が多いと考えられる. ただし, 第三者によって長時間の移動履歴が入手されるような場合, 第三者は *id* と実名との関連性を見出すことができる指摘されている [15]. それは個々のユーザのプライベートなエリア (ホームエリア) の存在があるためである. ある個人の家やその人のオフィスをおよそ決まった時間に行き来するような移動履歴が第三者にわたった場合, その位置情報に割り当てられている識別子は, その家の住民であると判断することができてしまう. このような点を考えると, 測位される識別子が実名でなく *id* だとしても, 十分にそのユーザ自身へのプライバシー侵害されるおそれのあることがわかる.

なお, 本稿においては上記の点を考慮して, 位置情報プライバシーの侵害を「第三者にユーザの位置情報が長時間にわたって不当に追跡されること」と定義する. これは文献 [15, 22] など定義されているものと同様のものである. 長時間の追跡でない限りは位置情報を発するユーザの実名が第三者に推測される危険性が小さいため, 長時間にわたって追跡されることがユーザのプライバシーにとって大きな問題であると考えている.

2.3 先行研究

プライバシー保護を議論する中で重要な概念に「匿名性 (anonymity)」といったものがある. 匿名性とはある一つの情報が, 誰によるものかが不明である状態をいう. そしてこの匿名性を実現するための一つの条件として「非結合性 (unlinkability)」といった性質があげられる. これは二つの情報がある場合に, その 2 つの情報の間

に相関が小さい場合に、非結合性が高い状態という。位置情報プライバシーの分野でいえば実名を推測し得るようなホームエリアでの位置情報の軌跡と第三者に知られたくないようなエリアで位置情報の軌跡との関係が不明であれば、知られたくないエリアでの軌跡の匿名性が確保され、ユーザのプライバシーを保護できるといえる。そのためには、長時間の追跡を回避する目的のもと、個々の移動軌跡の間の非結合性を確保していくことが必要であると考えられる。

このような匿名性の概念に基づいてプライバシー保護を試みる先行研究が匿名通信および位置情報サービスの分野で行われている。ここでそれらの概略を述べる。

まず匿名通信の分野であるが、匿名通信とはネットワーク上を流れているメッセージをみても送信者がだれなのか判断できないような通信形態をいう。電子投票や電子商取引、あるいは匿名投書などに用いられている。一般的な通信ではネットワークを監視する悪意のある第三者、つまり攻撃者によって容易にその送信者が推測されるような形態になっている。このような問題を解決するために 1980 年に Chaum は Mix-net と呼ばれるシステムを提案した [26]。これは図 2 のように受信者と送信者との間に MIX と呼ばれる中継サーバをたてて、この中継サーバが複数のメッセージをミックス（シャッフル）してかき混ぜることで、メッセージがどのように流れているかを隠蔽する手法である。中継サーバは入力されたメッセージと出力されるメッセージの関係を隠蔽することが目的となるが、その主な動作は、入力されたデータを別の形に変換（暗号化あるいは復号化など）すること、メッセージにランダムな時間遅延を与えることで、出力順序をランダムに入れ替えることの 2 点である。まず前者の動作によってデータの形から中継サーバ前後のメッセージの関係を推測されることを防ぐ。さらに後者の動作によってサーバ前後のメッセージの時間的相関を隠蔽することとなる。つまり入力されたメッセージと出力されたメッセージの間の非結合性を確保するための手法であるといえる。さらに実用の際には Crowds[28] に代表されるように単独の MIX ではなく、複数の MIX を直列に接続することでよりシステムの信頼性の向上をはかっている。

またこの分野においては匿名通信の匿名性を定量的に評価する手法としてアノニミティセット (Anonymity Set) といった概念を提案している [27, 30]。これは特定のメッセージに対してそのメッセージを送信する可能性のある送信者の集合である。特定のメッセージを追跡しようとする攻撃者にとってみれば、そのメッセージを送り得る送信者が 1 人しかいないような場合、容易にそのメッセージの送信者はそのユーザであると判断することができる。それに対して複数のユーザが送信し得る場合には誰がその特定のメッセージを送ったのか判断が困難になる。この

ように特定のメッセージに対して、それを送信し得る送信者が多いほど、そのメッセージが誰が送ったのか判断しにくい、つまりそのメッセージの匿名性が高いとすることができるため、匿名通信の信頼性を評価する定量的指標として、アノニミティセットのサイズあるいはその確率分布まで考慮したエントロピーといった値が用いられ、これらの値が大きいほど信頼性の高いシステムであるといえる。

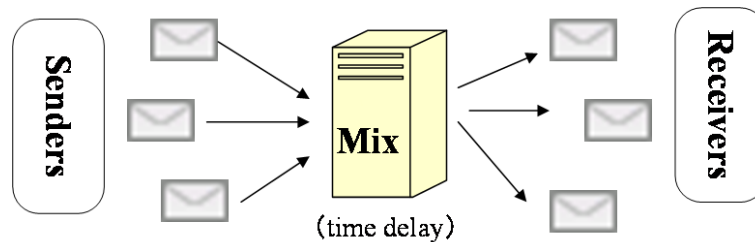


図 2: MIX in anonymous communication

一方、位置情報サービスの分野であるが、ユーザが位置情報サービスを享受したい場合、各サービスプロバイダーに自身の位置情報を公開しなければならない。信頼性の低いサービスプロバイダーに自身の位置情報を取得されることは大きな不安を伴ない、この分野においてもいかにユーザのプライバシーを保護するかといったことが議論されている。この分野で従来より多く提案されてきたものは主にポリシーベースのプライバシー保護手法である。ユーザが定めたポリシーに基づいて位置情報の公開の許可、あるいは位置情報の質などを適宜判断するといった手法である。たとえば就業中にのみ位置情報を公開し、仕事以外の時間には公開しないといったポリシーやどの街にいるか程度の粒度でのみ公開し、詳細な位置は公開しないといったようなポリシーを設定することができる。このようなポリシーベースの手法に対して、近年では匿名性を利用することによって常に位置情報を公開しながらも匿名でサービスを享受しようといった動きが高まってきた [15]。

匿名のままサービスを享受するシステムを実現するためには図 3 に示すようにユーザと個々のサービスプロバイダーとの間に、信頼性の高い機関の管理するミドルウェアをおく必要がある。ユーザは自身の所有する端末からこのミドルウェアにアクセスし、自身の ID と位置情報を公開する。ミドルウェアはその位置情報に何らかの擬似 ID (Pseudo ID) を割り振り、その PID と位置情報をセットにしてサービスプロバイダーに送信する。プロバイダーはその位置に応じたサービスをミドルウェアに返答し、ミドルウェアはさらにそれをユーザへとフィードバックするといった

動作形態をとる. ここで **PID** の取り扱いであるが, 固定の **PID** を用いていると長時間にわたりサービスプロバイダーがユーザの移動履歴を取得してしまうため, 定期的に **PID** を更新するとされている. つまり **PID** を可変とすることで長時間の追跡を回避している.

さらにユーザのプライバシーレベルを高めるために, 個々の **PID** を識別子として得られる各移動履歴の間の非結合性を高める提案もなされている. それらは基本的に個々の位置情報の品質を落とすことによって **PID** 更新前後の位置情報の相関が小さくなるといった考え方に基づいているものが多い. より詳細かつ正確な位置情報がプロバイダーに渡ることになると, 追跡される危険性が高まるからである. 具体的な手法としては測位できるエリアを制限する手法 [15] や位置情報の空間的粒度を調整する手法 [22] や時間的粒度を調整する手法 [20] などが提案されている.

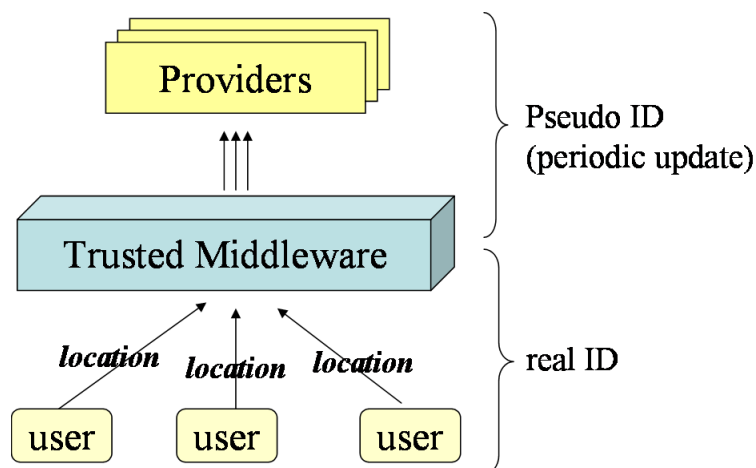


図 3: Architecture of location based service

3 無線通信端末における位置情報プライバシー

個人の位置情報プライバシーが脅威にさらされる環境の一つとして、ユーザが無線通信端末を利用する場合がある。本章においてそのような環境の概要を述べるとともに、いかにしてユーザの位置情報が漏洩するのか、攻撃者がいかにしてユーザを追跡することができるのかについてまとめる。

3.1 想定環境

近年、ユーザが持ち歩く小型 PC や PDA、そして携帯電話のようなモバイル端末にはネットワークにつなぐための無線通信機能が標準的に搭載されるようになった。ユーザがこれらのモバイル端末を所有していれば都市空間の至るところで無線通信ネットワークに接続し、サービスを享受することが可能なインフラ整備も進んでいる。アプリケーションとしては音声 (VOICE) や映像 (VIDEO) といったコンテンツをストリーミングして楽しむことも可能であるし、インターネットに接続して情報を得ることも可能である。

無線通信手法として代表的なものに無線 LAN (WLAN: Wireless Local Area Network) や Bluetooth といったものがある。無線 LAN は従来の有線の LAN で行われていた Ethernet と同様のことを無線に置き換えたものであり、1997 年に無線 LAN の最初の規格である [IEEE802.11] が IEEE (Institute of Electrical and Electronic Engineers : 米国電気電子技術者協会) によって取り決められたがはじまりである。Ethernet と同様にメディアそのものの仕様である物理層と、それを使って基本的なコミュニケーションを確立するための MAC (Media Access Control) 層の仕様がまとめられている。無線 LAN の特徴としては高速にデータ通信できることがある。近年では 5GHz 帯を使い最大 54Mbps の伝送速度を実現するような規格「IEEE802.11a」も一般化している。

一方、Bluetooth とは 1998 年にエリクソン・ノキア・IBM・インテル・東芝の 5 社により提唱された 2.4GHz 帯を使った近距離無線通信規格の名称であり、現在では Bluetooth SIG (Bluetooth Special Interest Group) によってさらなる議論が進められている。Bluetooth SIG とは Bluetooth に賛同した企業群であり、いまや 2000 社を超える企業がこれに参加している [17]。Bluetooth は基本的な通信距離が 10m 程度と短いいため、LAN に対して PAN (Personal Area Network) などと呼ばれることもある。最大伝送速度は 1Mbps と無線 LAN に比べて控えめな値となっているが、パケット

伝送方式とは別に音声通信用のプロトコルも搭載されており,PHS なみの音声通信も可能となっている.なお,Bluetoothのネットワーク形態はピコネットと呼ばれる形式をとる.これは通信半径内のエリアにおいて最初に通信を開始したデバイスが「マスタ」として動作し,その他のデバイスがこのデバイスにリンクを確立し「スレーブ」としてネットワークを構築する.このようなピコネットは最大7台までのデバイスが参加できる.さらにマスタは他のピコネットのスレーブとなることも可能のため,ピコネットを連結した形でスカッタネットを構築することも可能である.

従来,これらの端末のセキュリティに関する研究においてはデータプライバシーの侵害が対象とされてきた.図23のように基本的に無線通信端末を用いてサービスを享受する場合,都市空間に存在しているアクセスポイントに対して無線データ(無線パケット)を送信することによってそのアクセスポイント経由で種々のサービスを享受することとなる.しかしながら,この無線通信端末とアクセスポイントの間の通信が無線を介して行われるため,アクセスポイントとは関係のない第三者がこの無線パケットを受信(キャプチャー)することは容易である.このため,ユーザの行っている通信の内容,たとえばVOICEでの会話の内容などが,第三者に盗聴されてしまうことなどが危惧されてきた.これらのデータプライバシーの問題に関しては多くの暗号化技術などが提案され,研究が進められている.

それに対して近年,無線通信端末の利用に伴うユーザの位置情報プライバシー侵害の問題が指摘されるようになってきた[16].すなわちパケットをキャプチャーする第三者がユーザの位置を連続的に取得し,長時間にわたる移動履歴を取得してしまう可能性があるといことである.本研究においてはこちらの位置情報プライバシーの問題に関してまとめるとともにその解決手法を検討している.

3.2 攻撃者モデル

悪意のある第三者(攻撃者)はたとえ暗号化技術によって無線通信のデータが隠蔽されていたとしてもユーザの位置情報を取得することが可能である.本節においてはユーザの位置情報プライバシーを侵害し得る攻撃者モデルをまとめる.

まず攻撃者は都市環境中に複数のアクセスポイントを所有する.当然のことながら攻撃者にとってこのアクセスポイントの位置は既知の情報となる.これらのアクセスポイントは電波の通信半径内であれば,あらゆるユーザの無線パケットをキャプチャーすることが可能である.ユーザのパケットを送信する間隔はユーザの使用

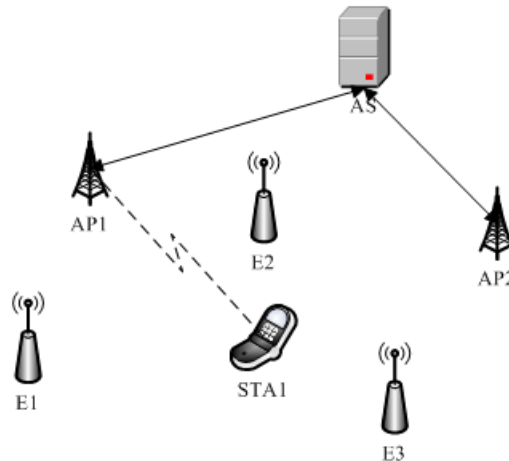


図 4: Wireless LAN system architecture

するアプリケーションのより様々であるが,VoIP などの場合 100ms 程度ごとに無線パケットを連続的に送信している. 本論文における攻撃者はこれらのパケットをすべて観察可能な攻撃者,いわゆる GPA(Global Passive Adversary) を前提としている.

次に攻撃者は得た無線パケットによってユーザの位置を推定する. 従来は無線 LAN あるいは Bluetooth を用いた測位といえば近接検知方式が主であった. すなわちどのアクセスポイントによってパケットがキャプチャーされたのかによって,そのアクセスポイントの近傍にユーザが存在していると判断する手法であった. この場合,位置情報の粒度は無線の通信半径に依存し,無線 LAN の場合は 100m,Bluetooth の場合でも 20m 程といった程度であった. しかし信号処理技術の発達に伴ない,近年では無線パケットの物理量(電界強度、到達時間)の情報に基づいた三点測量方式の測位手法が一般的に用いられるようになった. このため攻撃者の得られる位置情報の質は大きく向上し,無線 LAN, Bluetooth とともに誤差数 m 程度の測位も可能となっている [3, 4, 5].

さらにこれらの位置情報には識別子として MAC アドレスがふられている.MAC アドレスとは各モバイル端末に割り当てられたユニークなアドレスであり,各無線パケットのヘッダ部分に記載されている. このヘッダ部分の情報は正当なアクセスポイントが認証のために利用するために,データ部分が暗号化されていてもこの部分は暗号化などされていない. そのため暗号化されたデータは攻撃者には読みとることができなくても,この MAC アドレスを読みとることは可能である. 攻撃者は同一の識別子(MAC アドレス)で位置推定された位置を結合させることによって,特

定のユーザの長時間にわたる移動履歴を得ることが可能となる。

このような長時間に渡る追跡を回避するために WLAN, Bluetooth とともに既にいくつかのプライバシー保護手法が提案されている。それらは固定の MAC アドレスに問題の焦点をあて、この MAC アドレスを定期的に更新することを基本としている。つまり攻撃者によって取得される位置情報のうち識別子を可変とすることで、長時間にわたる追跡を回避するのである。無線 LAN においては文献 [16] で使い捨ての MAC アドレスを使用することが提案され、アドレス重複の問題などその機構が検討されている。また Bluetooth においては Bluetooth SIG が Anonymity mode と呼ばれるモードの中で使い捨ての MAC アドレスを使用することの規格化の議論などが行われている [18]。

従来のように粒度 100m 程度といったような位置情報しか測位しかできない環境においてはこれで十分だと考えられてきたが、近年のように高精度な測位が可能であり、かつユーザが頻繁にパケットを送信するような環境においては、単純に MAC アドレスを定期的に変えるだけでは十分ではないと我々は考えている。攻撃者は同一ユーザによって応答される、異なる id の位置情報 $(id, s, t), (id', s', t'), \dots$ との間に何らかの相関を見出すことでそれらの複数の位置情報を再結合し、そのユーザの長時間にわたる移動履歴を取得することが可能となる。具体的な位置情報の相関の例には下記のようなものが挙げられる。

(a) アドレス自身の相関

理想的にはアドレスを更新する際には更新前後のアドレス自身には相関が皆無である状態が望ましい。しかし実際には用いるアルゴリズムによっては相関が残る場合が考えられる。またアドレスを管理しているデータベースの情報などが攻撃者に漏れた場合のも、複数のアドレスが同一端末に属しているものだと容易に判断されてしまうおそれがある。

(b) 時間的相関

測位間隔などの影響により、同一ユーザの新しいアドレスでの位置情報は、古いアドレスで最後に測位された時間から一定時間内に出現すると考えられる。その時間内に他のユーザの位置情報が観測されないような場合、容易に追跡することが可能となる。

(c) 空間的相関

移動速度などの影響により、同一ユーザの新しいアドレスでの位置情報は、

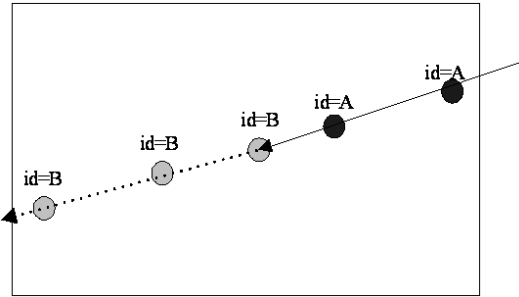


図 5: The correlation attack on periodical address update

古いアドレスで最後に測位された場所を基準とした一定のエリアに出現すると考えられる. そのエリア内に観測される他のユーザの位置情報が少ないような場合には, 容易に追跡することが可能となる.

このような相関がある限り, 同一ユーザの異なる識別子の位置情報の非結合性が十分に確保されない. そのため識別子を更新したとしてもユーザの位置情報プライバシーが侵害される危険性がある. 本論文においてはこれらの相関のうち, 特に時間的・空間的相関を利用した追跡問題に着目し, それに対して位置情報プライバシー保護手法を検討している. なお, ここではアドレス自身の相関はないものと仮定して議論を進めている.

図 5 には時間的・空間的相関の一例を示す. 高精度かつ高頻度の測位環境においてユーザがアドレス A を使いながら右側から移動してきて, 途中でアドレス B へと更新している. アドレス A で測位された最後の位置情報は (DP, DT) , 新しいアドレス B で最初に測位された位置情報は (EP, ET) である. 識別子だけみる限りはこれらの 2 つの移動軌跡は異なるユーザのものであるが, 攻撃者はこの 2 つの移動軌跡の時間的・空間的相関を見出し, 関連づけることで 2 つの軌跡を再結合し, このユーザのより長時間にわたる移動履歴を得ることができる. 具体的な追跡手法に関しては次節において述べる.

3.3 追跡アルゴリズム

本節では 2 つの識別子の位置情報の時間的・空間的相関を利用した追跡手法について考察する. ここで言葉として, 攻撃者が測位可能な複数のユーザの中で, 攻撃者が追跡しようとしているユーザを **target**, その他のユーザを **mixer** と呼ぶこととする. つまり, ここで検討する追跡手法は言い換えれば, 攻撃者が **target** がアドレ

スを更新した際に, mixer の存在に惑わされず target の新しいアドレスでの位置情報を見つけ出すことのためのアルゴリズムであるといえる. 本論文においては既存の追跡手法などを参考に 3 つの具体的な手法を述べる.

(1) Simple tracking

これはターゲットの最後に測位された位置情報と時間的・空間的相関が 0 でないすべての他の位置情報の中からランダムに一つを選び出し target の位置情報であると判断するアルゴリズムである. ここで「相関が 0 でない」といった具体的な判断基準は 4.2 節にて詳細を述べるが, 簡易的に空間的な観点から述べた図を図 6 左に示す. 図中の $P(id, time)$ は連続的に測位されているノードのアドレス id , 時間 $time$ の場所を示しておりアドレスを T から T' へと変更しているノードが target であると考え. 攻撃者にとってみれば, T で測位された最後の位置情報 $P(T, t-1)$ を基準として一定のエリア内に target の新しい ID での位置情報があると考えることができる. このエリア内に $P(T', t)$ のターゲットの位置情報しかないような場合には攻撃者は容易にターゲットの新しいアドレスが T' であると判断することができるが, $P(M', t)$ のように同様な時間帯に測位されている mixer の位置情報がある場合には, ターゲットの新しいアドレスが T' であるのか M' であるのかの判断が困難になる. ここでは無作為に判断するとしているので, もしエリア内に n 個の位置情報 (target の位置情報を含む) があるような場合, 攻撃者は正確に追跡できる確率は $1/n$ であるといえる.

(2) Correlation tracking

空間的な相関には, 単純に 2 つの位置情報の距離が小さいという関係だけでなく, 連続した位置情報がユーザの移動モデルによく合致している場合もある. 一般に人が都市環境を移動する際には一定速度で直進的に進む場合が多い. そこで攻撃者がこのような移動モデルの情報を知っており, かつ比較的高精度な測位が可能であれば, この直進性を利用した追跡が可能となる. このようなユーザの移動の直進性を利用した追跡手法を Correlation tracking と呼び, 図 6 右に示す. 攻撃者はまず古いアドレスでの位置情報の測位履歴より, 新しいアドレスで測位されるであろう位置 P_{est} を推測する. 本論文においては簡易的に測位履歴のうち 2 つの位置情報を用いてその直線上に P_{est} を推測すると仮定する. そして攻撃者は複数の位置情報 $P(T', t)$ や $P(M', t)$ などが存在していてもこの P_{est} にもっとも近い位置情報をターゲットの位置情報であると判断するものとする.

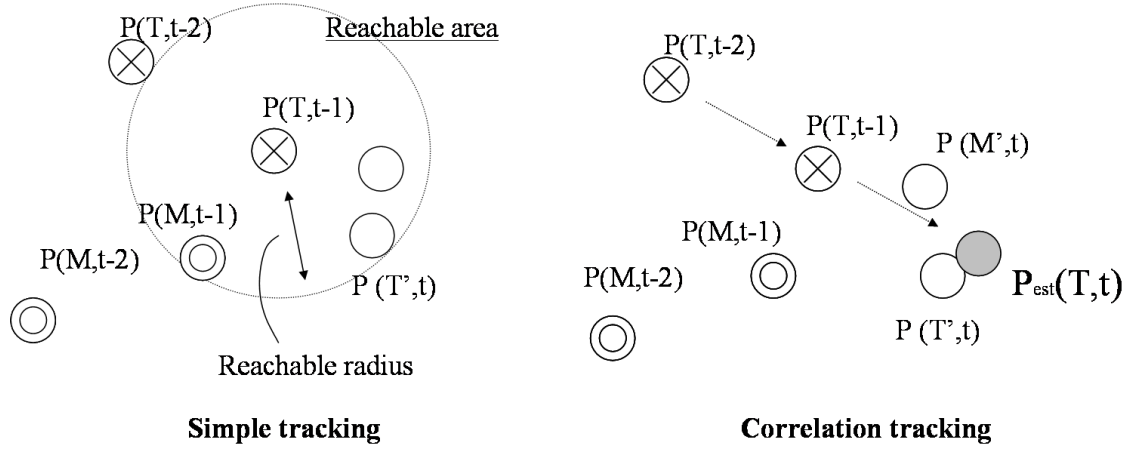


図 6: Tracking method (Simple/Correlation tracking)

(3) Kalman tracking

実際に攻撃者によって取得される位置情報には当然, 誤差が含まれる. この誤差が大きいような場合, Correlation tracking の手法で P_{est} を予測しても, 実際の target の位置と大きく異なる場合が多い. そこで一般的な追跡システム [7] においても使われることの多い Kalman filter を用いることで, この推定誤差を軽減することができる. P_{est} を予測した後は Correlation tracking と同様にもっとも近い位置情報を target のものと判断するものとする. Kalman filter の用いる際には, 現在の状態と過去の状態がどのような関係にあるのかを示すプロセスモデルと, 現在の状態がどのように測定されるのかを示す測定モデルとを定義しなければならない. ここでは文献 [6] に従ってそれらを定義した. まず位置情報における状態 X_k とは 2 次元位置 x, y とそれぞれの軸方向の \dot{x}, \dot{y} の 4 つの要素からなると考えられる. そしてある時点での状態 X_k は行列 F_k を介して直前の状態 X_{k-1} にのみ依存すると仮定した中で下記のプロセスモデルが定義される. なお W_k は本モデルに当てはまらないプロセスモデルにおけるノイズである.

Process model : $x_k = F_k x_{k-1} + w_k$

$$\begin{pmatrix} x_k \\ y_k \\ \dot{x}_k \\ \dot{y}_k \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_{k-1} \\ y_{k-1} \\ \dot{x}_{k-1} \\ \dot{y}_{k-1} \end{pmatrix} + \begin{pmatrix} w_k^x \\ w_k^y \\ w_k^{\dot{x}} \\ w_k^{\dot{y}} \end{pmatrix}$$

測定モデルに関しては, 測定される情報 Z_k は 2 次元の位置 z_k, z_y の 2 要素から構成される. Z_k はユーザの位置にのみ依存し, 速度には依存しないという仮定のもと

で以下の測位モデルが定義される. なお V_k は本モデルにあてはまらないノイズ, つまり測位誤差である.

Measurement model : $z_k = H_k x_k + v_k$

$$\begin{pmatrix} z_x \\ z_y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_k \\ y_k \\ \dot{x}_k \\ \dot{y}_k \end{pmatrix} + \begin{pmatrix} v_k^x \\ v_k^y \end{pmatrix}$$

以上のようなプロセスモデル, 測定モデルを定義した. このような Kalman filter を用いることで, 図 7 に示すように移動履歴がスムージングされ, より精度の高い P_{est} を予測することが可能となる.

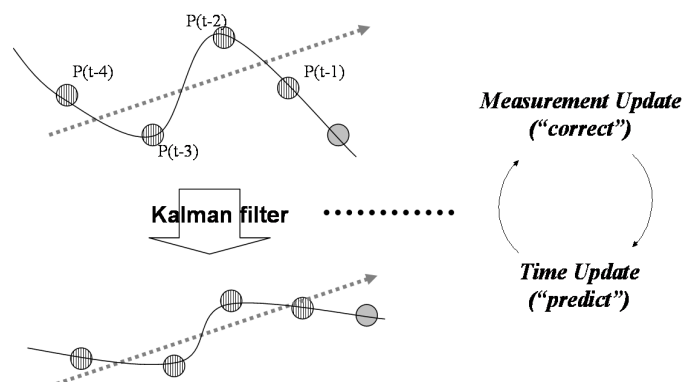


図 7: Illustration of Kalman Tracking

4 Silent period の提案

本節においてはプライバシー保護手法として **silent period** という手法を提案する. またその手法の有効性を示すための評価方法を検討し **GAS** といった概念および **MTR** といった位置情報プライバシーの定量的指標を提案する. 最後にそれらの評価指標に基づき **Silent period** の評価を行った結果を示す.

4.1 Silent period

前節で考察したような時間的・空間的相関を利用した攻撃者に対して, ユーザの位置情報プライバシー保護するために, 我々は **silent period** と呼ばれる手法を提案する. 一般的に言えば, これは更新前後の位置情報の非結合性を高めることによってユーザの位置情報の匿名性を高める手法である. **Silent period** は古い ID から新しい ID への移行する期間であり, かつその間は無線端末は一切通信を認められない期間である. このような **silent period** を設けることにより, ID 更新前後の位置情報の関係が曖昧になる, つまりそれらの間の時間的・空間的相関が小さくなると考えられる. このことは攻撃者にとってみれば, 特定のユーザを追跡することが困難になると考えられ, ユーザの位置情報プライバシーが保護されると期待される.

Silent period の例を図 8 に示す. 図中には 2 つのユーザを示しており, ユーザ 1 が右上から左下に移動し, ノード 2 は右下から左上に向けて移動している. 両方のノードが **Silent period** の期間を経てそれぞれの ID を更新している. ノード 1 は $ID : A$ を用いて通信を行っていた中で, 時刻 DT_1 , 場所 DP_1 において **Silent period** に入り, 通信を中断し, 続く時刻 ET_1 , 場所 EP_1 において $ID : A'$ を用いて通信を開始している. 同様にノード 2 は $ID : B$ を用いて通信を行っていた中で, 時刻 DT_2 , 場所 DP_2 において **Silent period** に入り, 時刻 ET_2 , 場所 EP_2 において $ID : B'$ を用いて通信を開始している. ここで 2 つのノードは時間的に同時に **Silent period** に入ることを仮定している ($DT_1 = DT_2$). 攻撃者の目的は, たとえばユーザ 1 を追跡しようとしている場合, (DT_1, DP_1) と (ET_1, ET_1) との位置情報相関を見出し, それらの 2 つの位置情報が同一ユーザに属していると判断することとなるが, **Silent period** が長いほどその 2 つの位置情報は時間的に空間的にも離れた情報となる. このことによってユーザ 1 の新しい位置情報が (ET_1, EP_1) なのか (ET_2, EP_2) なのか判断が難しくなると考えられる.

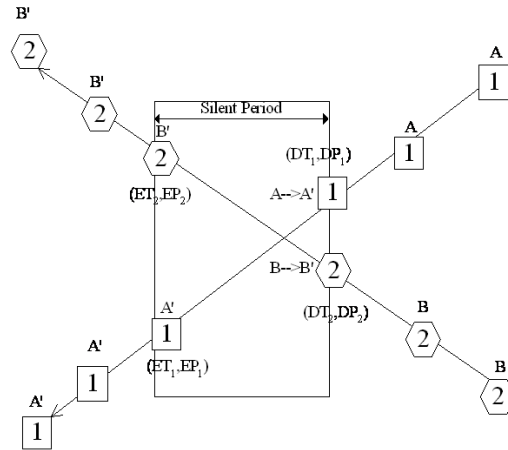


図 8: Illustration of Silent period

4.2 評価手法の検討

本節においては **Silent period** によってもたらされるプライバシーレベルを定量的に評価・解析をおこなうための手法を検討する. そのために我々は匿名通信における評価手法を参考にしている.

そもそも 2 章において述べた匿名通信における **MIX** と呼ばれる手法と, 位置情報プライバシーにおける **Silent period** の手法は類似している部分が多い. 前者は送信されたメッセージと受信されたメッセージの相関を隠蔽するために, その間にランダムな遅延に基づく時間的な曖昧さを発生させて, その相関を小さくしている手法であるといえる. つまりメッセージ間の非結合性を高めることによりメッセージの匿名性を実現している. ただしこの場合, 相関とは時間的な相関のみを意味する. それに対して位置情報プライバシーの場合は, **ID** 更新前後の 2 つの位置情報の相関を隠蔽するために, 通信できない時間を設け, その相関を小さくしている手法である. つまり位置情報間の非結合性を高めることによって, ユーザの位置情報の匿名性を実現している. そしてこの場合の相関とは時間的相関だけでなく, 空間的な相関まで含まれる.

このような両者の類似点に着目し, 我々は匿名通信における匿名性の評価手法であるアノニミティセットの概念を, 今回の位置情報プライバシーの評価に応用することを考えた. 2 章で述べたようにアノニミティセットは「特定の受信されたメッセージと時間的に相関のある (時間的な相関がゼロでない) 送信メッセージの集合」である. これに対して位置情報プライバシーの場合, 時間的相関だけでなく, 空間的相関も考慮しなければならないため, 我々はアノニミティセットの概念を拡張

し,GAS(Geographical Anonymity Set) と呼ばれる概念を提案する. これは「ある位置情報と時間的・空間的に相関のある他の位置情報の集合」と定義される. ターゲットの古いアドレスで最後に測位された位置情報とその周辺の他のノードとの相関を調べることによって GAS に含まれる位置情報を判断し, この集合を形成する. この集合により多くのノードが含まれている場合, 攻撃者にとってターゲットの新しいアドレスの位置情報を見出すことが困難になり, ユーザの位置情報プライバシーは向上するといえる. ここで GAS のサイズあるいは確率分布まで考慮したエントロピーを位置情報プライバシーの定量的評価に用いることができる.

時間的・空間的な相関の有無の判断には **Detection window(D_w)** および **Reachable radius(R_r)** といった値を定義し使用する. 特定のユーザのある位置情報が測位されてから, 同じユーザの位置情報が測位されるまでの時間は **silent period** の長さ, ユーザの使用しているアプリケーションのトラフィックモデルなどに影響をうけて固定の値ではないが, ある一定時間におさまると考えられる. **Detection window** はこの閾値を定義したもので, ある位置情報が時間 t に測位された場合, その位置情報と時間的に相関のある他の位置情報とは時刻 t から時刻 $t + D_w$ の時間までの期間に測位された位置情報であるといえる (図9左). 同様に空間的な観点からも, 同一ユーザの連続した二つの位置情報の距離はユーザの移動速度, 測位間隔などの影響から一定の値におさまると考えられる. **Reachable radius** はこの閾値を定義したもので, ある位置情報と空間的に相関のある他の位置情報とはそれらの間の距離が R_r より小さいものであるといえる (図9右). 以下に GAS を計算する際の擬似コードを示す. すべての Mixer の位置情報 (EP_i, ET_i) に対して Target の位置情報 (DP, DT) との時間的相関, 空間的相関のそれぞれをチェックし, 両者ともに相関のある位置情報を GAS に含まれるものとしてカウントしている.

Definition:

DP,DT: Location information of target (position & time):

EP(i),ET(i): Location information of i mixers (position & time):

Function check_SpaceOverlap(DP,EP){

If Distance(DP,EP)<Reachable radius, **Return** TRUE

else, **Return** FALSE;

}

```

Function check_TimeOverlap(DT,ET){
  If  $0 < ET - DT < \text{Detection Window}$ , Return TRUE;
  Else, Return FALSE;
}

Function calculate_GAS{
  Foreach (ET(i),EP(i)){
    If check_SpaceOverlap(DP,EP(i)) is TRUE
      and check_TimeOverlap(DT,ET(i)) is TRUE, C++;
  }
  Return C;
}

```

なお, この detection window, reachable radius の値は評価しようとする環境によって変化するものであるので, 今回の評価においてはそれぞれの環境において事前のシミュレーションを行い求めるものとする. まずある一定の環境の中で複数回のシミュレーションを行うと, 複数の位置情報に対して, 連続する2つの位置情報の時間差分 Δt と距離 D が求められる. 具体例として図 10 左にはユーザが 1s 間隔でパケットを送信しながらエリア内をランダムに移動する (移動モデルはランダムウォーク) 中で誤差 0.5m の場合と 1.5m の場合の距離データのヒストグラムを示した. ユーザの移動速度は 0.5m/s ~ 1.5m/s としている. 誤差を考慮しないような場合には距離 D の値は 1 秒間隔で測位されているため $1 \times 1.5 = 1[m]$ の値を最大値とするのだが, 今回のように誤差がある場合, 誤差の影響によってその値を超えるような場合もある. 図 10 左より誤差が大きいほど距離 D の分布は広がることも分

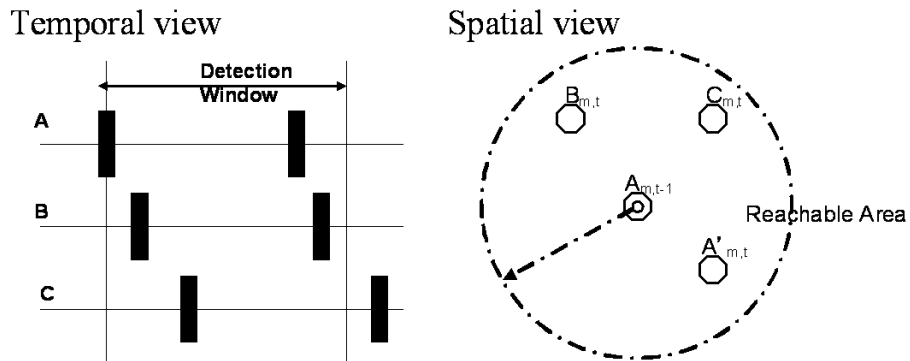


図 9: Spatial and Temporal view in Geographical Anonymity Set

かる. このヒストグラムのデータを図 10 右のような累積分布関数 (CDF: Cumulative Distribution Function) に落とし込み, その累積確率が 1.0 に近い値 (本研究においては 0.98) となる際の距離 D を閾値, つまり Rr として決定する. 時間的な Dw に関してもまったく同様なことを行うとする.

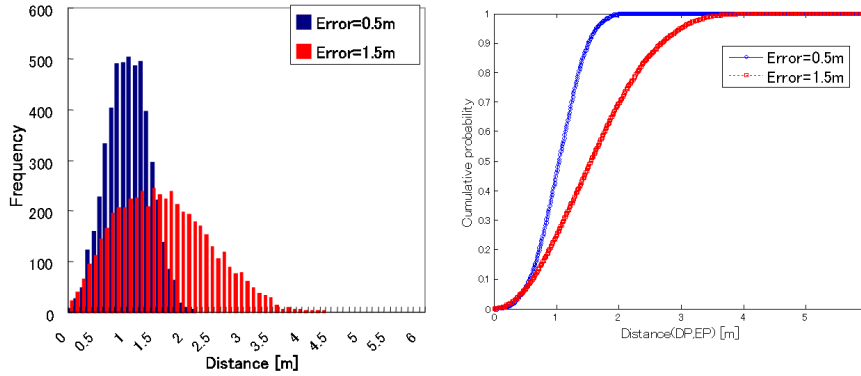


図 10: Histogram and CDF of distance data

GAS の概念はプライバシーの定量的評価に有効に使えるが, この概念だけでは攻撃者の用いる追跡手法の上でのプライバシーの脅威を評価しきれない. すなわち GAS の評価対象になるのは時空間的・空間的な相関の有無であり, ユーザの移動モデルを利用したような追跡手法である **correlation tracking**, **Kalman tracking** などの影響を評価するのは困難である. そこで, これら追跡手法の影響を直接的に定量評価するために最大追跡回数 (**MTR: Maximum Tracking Round**) といった評価関数を用意した. これはユーザが定期的にアドレスを更新していく中で, ユーザにとってみれば何回の更新の後に追跡を免れることができるのか, 攻撃者にとってみれば何回の更新まで正しく **target** を追跡できるのかといった回数を示す値である. 同様な GAS が確保されるような環境においても攻撃者がより高度の追跡手法を用いることによってこの MTR の値は大きくなるものと考えられる.

4.3 評価

GAS の概念および MTR といった評価指標を用いて, 位置情報プライバシーの評価を行った. 評価は主にシミュレーションによって行った. 一定のシミュレーションエリア内を複数のノードが移動していると想定した. ノード数は常に一定とし, 各ノードが通信トラフィックモデルに基づいた通信を行っている. ここでの移動モデルは **Random Waypoint** モデルを利用した. **Random Waypoint** モデルはモバイルネット

表 1: Simulation Configuration for evaluating silent period

Parameter	Value
Simulation Area	20m × 20m
Mobility model	Random waypoint (Speed = 0.5-1.5 m/s)
Init position of node	Uniform distribution
Traffic model	Periodic transmission (interval=0.5-4.0s)
Tracking method	Simple/Correlation/Kalman tracking
Number of nodes	50-200
Positioning error	0.0-3.0m (Uniform distribution)
Silent period	0.0-5.0s

ワークなどのシミュレーションに頻繁に用いられる移動モデルの一つであり [39], シミュレーションエリア内に目的地をランダムに選び出し, その点に向かって一定の速度で移動する.そしてその目的地に到達すると一定時間 (**Pause time**) その点に留まり, また新たな目的地, および移動速度を決めてその点に向かって移動するといった移動モデルである. 本シミュレーションにおいては **Pause time** は 0 と仮定し, 移動速度は 0.5-1.5[m/s] の間の一様分布とした. トラフィックモデルに関しては簡易的に一定間隔で定期的に無線パケットを送信するような場合を想定した. 攻撃者はユーザが通信を行うたびにパケットをキャプチャーし, ユーザの位置情報を取得できる環境にある. ユーザは **silent period** を用いて自身の ID を更新し, 攻撃者は前述したような 3 つ追跡手法をもちいて追跡を試みる. なお, 今回は各ユーザが同期してアドレスを更新すると想定している. なぜなら, 今回の想定環境の場合, エリア内に存在する正当なアクセスポイントがそのような同期制御を行うことが可能だと考えられるためである. 以上のような中で **GAS** のサイズ・エントロピーあるいは **MTR** の値を定量的評価の指標として用いて評価を行った. シミュレーション環境の主なパラメータを表 1 にまとめる.

以上のような環境においてシミュレーションを行った結果を以下に示す.

まず, 図 11 は **GAS** の概念において位置情報プライバシーレベルを評価した結果である. 図 11 左は横軸にノード密度, 縦軸に **GAS** のサイズをプロットしている. また図中の直線がシミュレーションの結果である. この図よりノード密度が大きいほど **GAS** のサイズが大きい, つまり匿名性が向上していることがわかる. これはター

ゲットの **Reachable Area** に含まれるノード数がノード密度に比例して大きくなるためだと説明できる. また今回のように同期してアドレスを更新し, 誤差を考慮しない場合には幾何学的な計算によって **GAS** の値を求めることができる. 図中の点線はその理論値を示している. 誤差を考慮しない場合には Rr の値は速度 v と測位間隔 Δt によって決まる. すべてのノードが同期してアドレスを更新するような場合, 時間的相関の判断は不要であり, 一定のエリア内で半径 Rr の円の中に含まれるものが **GAS** の集合となるため, そのサイズは以下の式で与えられる. ただし D はノード密度を示している.

$$GAS = \pi \times D \times (v \times \Delta t)^2$$

図 11 右は測位誤差と **GAS** のエントロピーとの関係を示している. 2つの曲線はそれぞれ **Simple tracking** と **Correlation tracking** の場合を示している. まず測位誤差が大きいほどエントロピーが大きくなっていることがわかる. いいかえれば精度良く測位されるような環境にある場合, ユーザの位置情報プライバシーは侵害されやすい. また攻撃者がより高度な追跡アルゴリズムを用いる場合, ターゲットはより追跡されやすくなるといえる.

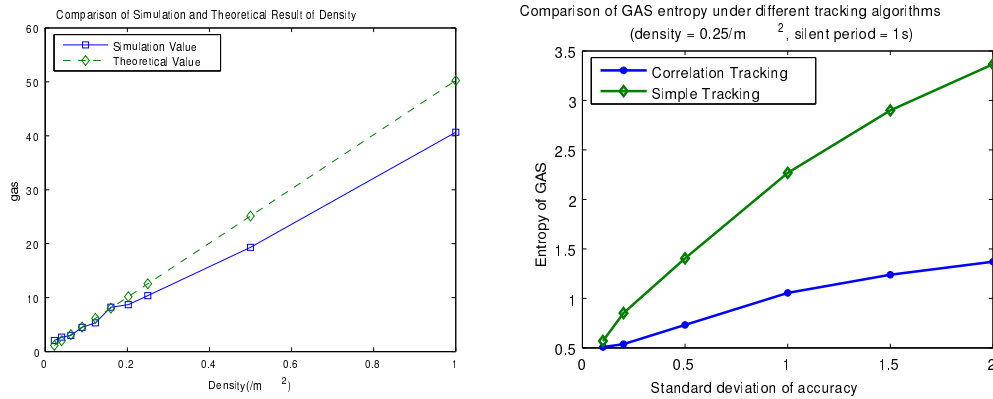


図 11: Evaluation based on Geographical Anonymity Set

図 12 には **MTR** を評価指標とし, 3つの追跡手法を比較した場合の結果を示す. 図 12 左は横軸にノード密度を, 図 12 右は横軸に測位間隔を示している. なお, 測位間隔とは今回の想定では無線端末が通信を行う間隔に等しい. まず図 11 と同じくノード密度が大きいほど追跡される回数が小さくプライバシーレベルが向上していることが分かる. また測位間隔が長いほど追跡されにくいこともわかる. さらに **Simple tracking**, **Correlation tracking**, **Kalman tracking** の順により追跡されやすい状

況になっている. 図 12 右で測位間隔が長い場合に **Correlation** と **Kalman** が逆転しているが, これは多くのサンプリングの点を用いてフィルタリングする必要のある **Kalman tracking** が有効に動作していないためだと考えられる.

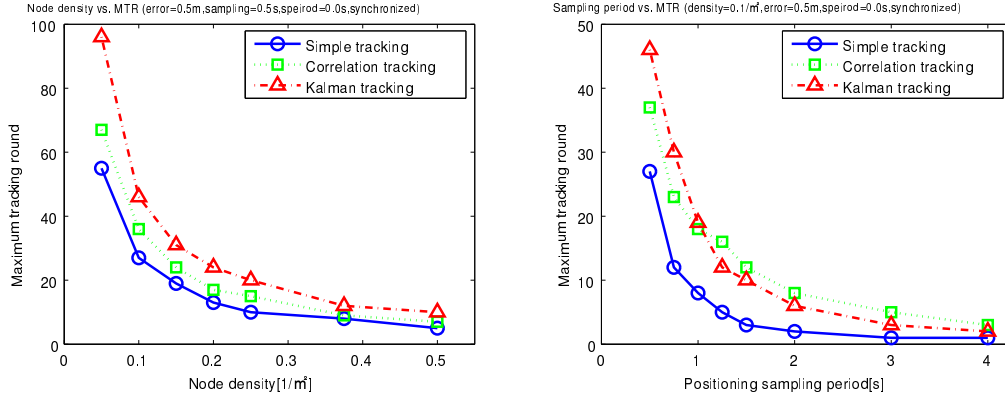


図 12: Evaluation based on Maximum Tracking Round

最後の我々の提案する **silent period** の有効性を評価した結果を示す. 図 13 左は横軸に **silent period** の長さを、縦軸に **GAS** のサイズをとったものである. **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. また図 13 右は縦軸を **MTR** として 3つの追跡アルゴリズムを比較したものである. すべての追跡手法に対して **silent period** が有効に働いていることがわかる.

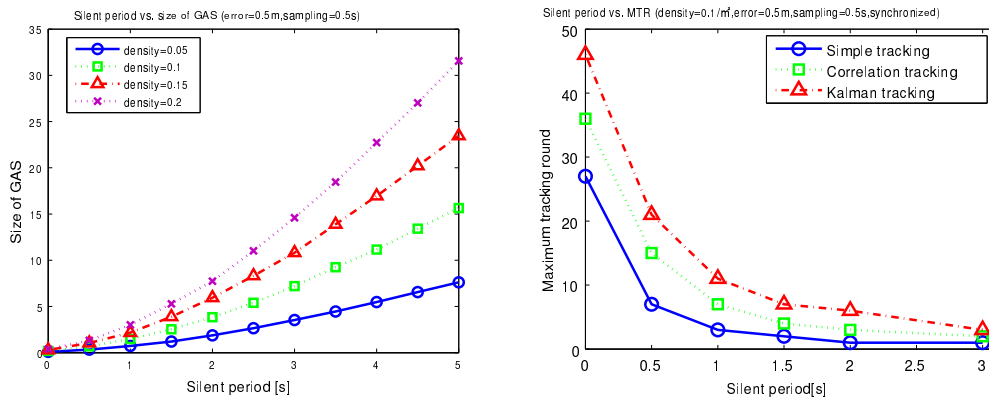


図 13: Evaluation of silent period

以上シミュレーションの結果より, 密度が大きい, 誤差が大きいほど高く, 追跡アルゴリズムが高度であるほど低くなることがわかった. また **Silent period** によって匿名性が向上したことがわかった.

5 Silent cascade の提案

前章の評価・解析の結果より,長い silent period を設けることで,十分な GAS を保障でき,プライバシー保護に有効であるといった見解を得た.しかしながら silent period の増加は通信不可能な期間の増加につながるためユーザが使用する無線通信サービス (アプリケーション) の品質に大きな影響を及ぼす.つまりユーザの位置情報プライバシーとアプリケーションのサービス品質 (Quality of Service,QoS) との間にはトレードオフの関係が存在しており,silent period の手法を実用するためにこの問題を考慮しなければならない.本章においてはまずアプリケーションの特性に基づいて QoS に関してまとめた後,Silent period を拡張した Silent cascade といった手法を提案し,その評価・解析を行う.

5.1 QoS とプライバシー

QoS とはサービスを使用しているユーザの満足度を決定するサービスの品質のことであり,通信システムを構築する際にはこの QoS が向上するような設計を行うことが求められる.このアプリケーションにおける QoS を具体的に議論する際にはアプリケーションごとの通信トラフィックの特性を考慮しなければならない.無線パケットの発生する頻度に着目すると多くのアプリケーションはリアルタイムアプリケーションとノンリアルタイムアプリケーションの2つに大きく分けることができる.リアルタイムアプリケーションとは時々刻々と発生する無線パケットを連続的に送信するようなアプリケーションであり,後者はパケット送信の必要が生じたときにバースト的にパケットを送信するようなアプリケーションのことである.

リアルタイムアプリケーションの例としては音声や映像のストリーミングを行うようなものがあげられる.近年では IP パケットによって音声を通信する VoIP (Voice over IP) といったものも一般化してきている.具体的な通信トラフィックに目を向けると文献 [23] によれば, VoIP の場合は基本的には 60ms といった微小時間間隔で通信を行うことが望まれる.データ通信の遅延は QoS の劣化に直結するため,このようなアプリケーションを使用している間に長い silent period を設けてアドレスを更新することは難しいといえる.たとえば VoIP であればユーザによって許容され得る片方向遅延として 200ms という値も報告されており [24],これより長い値の silent period を設けることは QoS へ大きな損失を与えられとされる.

一方、ノンリアルタイムのアプリケーションとしては HTTP に基づくウェブ閲覧や FTP に基づくファイル転送などが挙げられる。これらのアプリケーション場合、ユーザがデータ通信の要求を出す時（たとえばウェブページを移動する時など）にのみバースト的な通信パケットが発生し、それ以外の時間にはパケットが発生しない。つまり **silent period** がこのパケットの発生する時間帯に重複しない限りは、比較的長い **silent period** も許容される。アプリケーションの QoS に影響を与える要素としては遅延ということよりは、通信を正常に行える時間の比率、つまりユーザがデータ通信を要求した際に **silent period** でない確率といったものが大きな要素となると考えられる。

図 14 には QoS とプライバシーのトレードオフの関係を概念的に示す。横軸にサービスの品質、縦軸にプライバシーのレベル、つまり匿名性をとった場合に図中の曲線はそれらの間のトレードオフの関係を示す。QoS の制約が弱いような場合には見たすべきプライバシーレベルと QoS との両立が可能となるが、リアルタイムアプリケーションのように QoS の制約が強いような場合にはプライバシーレベルとの両立が達成できなくなるといったことがいえる。

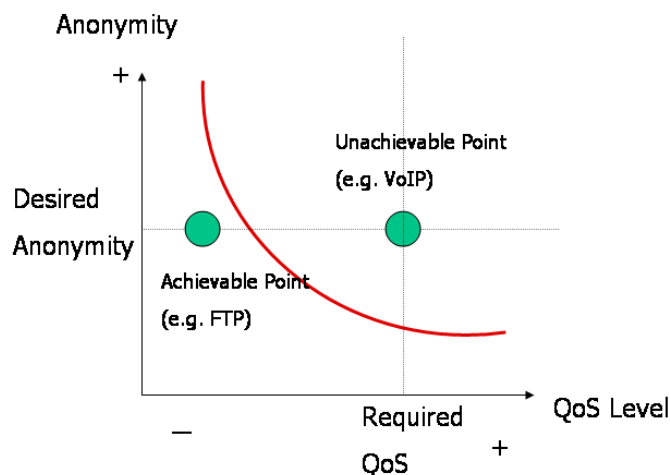


図 14: Trade-off between privacy and QoS

5.2 Silent cascade の提案

QoS の制約が強いような場合においても一定のプライバシーレベルを実現するための手法として、我々は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

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．この手法を **Silent cascade** と呼ぶ．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．十分な連鎖の段数を確保することができれば，この手法により **QoS** の制約を満たしつつも，位置情報プライバシーを保障することが可能となる．

匿名通信における **Mix-cascade** と，位置情報プライバシーにおける **Silent cascade** の概要を図 15 に示す．これらを比較した場合に，**Silent cascade** の特徴として連鎖の段数の制限が緩和であるといったことが挙げられる．

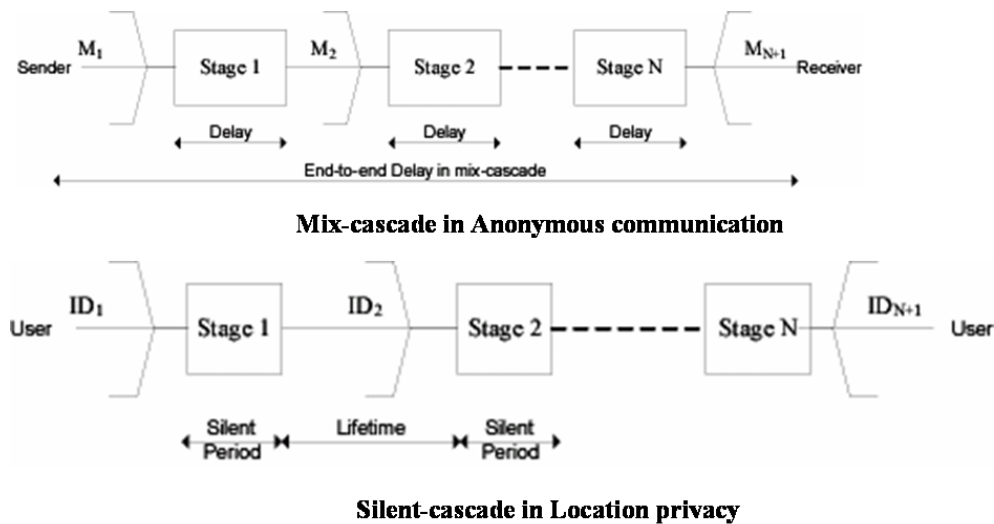


図 15: Comparison between Mix-cascade and Silent-cascade

Crowds[28] に代表されるような匿名通信における **Mix-cascade** の場合，目的はデータの送信者と受信者との間の匿名性を保障することにある．そのために送信者と受信者の間で複数の **MIX** にパケットを仲介させる．各ステージの **MIX** はパケットを受けるとランダムな時間だけ待ち時間を挟み，次のステージの **MIX** へとパケットを転送する．待ち時間があることによって **MIX** に入ってくるパケットと出ていくパケットの間の時間的相関を小さくしている．多くの段数が確保されればプライバシーレベルが向上するが，当然のことながらデータ伝送の遅延も増大することとなる．匿名通信においては段数を決定する際に，この遅延とプライバシーの相反する要求を考慮することが重要な問題となっている

それに対して，位置情報プライバシーにおける **Silent cascade** の場合，目的はユーザが追跡から逃れるために更新する識別子 (**MAC** アドレス) の匿名性を確保するこ

とにある．図 15 の下段に示したように，ユーザは ID_1 を用いて通信を行っている中で，プライバシー保護のために Mix-cascade のステージ 1 に入る．そして ID_1 から ID_2 に更新するとともに，silent period の時間だけ通信を遮断し， ID_1 と ID_2 の時空間的相関を小さくする．Silent period の時間が経過すると ID_2 を用いてまた通信を再開する．なお，本プロトコルにおいて同一の ID を使い続ける期間を Address lifetime と定義している．以上のようなことを再帰的に行い最終的に N 段の段数を経て， ID_{N+1} と ID_1 との間の非結合性が保障されることとなる．ユーザにとってみれば，silent period 以外の期間に正常に通信が行えるのであれば，Mix-cascade の段数といった要素は QoS には影響を及ぼさず，プライバシー保護のためには，段数に制限を設ける必要がないといえる．

評価・解析に関して考えてみると，文献 [29] によれば，Mix-cascade は以下の公式により評価される．ユーザが N 個の直列に接続された MIX 通過する場合，Mix-cascade により生み出されるアノニミティセットのサイズおよびエントロピーは以下の式で表される．Mix-cascade の段数を n ，各段におけるアノニミティセットのサイズおよびエントロピーを S_i ， E_i としている．

$$\Theta_n = \prod_{i=1}^n S_i \quad (1)$$

$$\Lambda_n = \sum_{i=1}^n E_i \quad (2)$$

この数式に基づき，Mix-cascade の場合，段数 n が決定されれば GAS のサイズあるいはエントロピーで定量的な評価が可能となる．しかしながら Silent cascade の場合，その段数の値はかなり大きな値，場合によっては無限大が許容されるため，ユーザが享受できるプライバシーレベルもまた無限大であるといった場合がある．ユーザの立場からすれば，繰り返しアドレスを更新していれば，どれだけ時間がかかろうと，最終的には元のアドレスと新しいアドレスの時空間的相関をなくすることができるといったことになるが，これではプライバシーレベルの解析を行う際に困難が生じる．

そこで本章においては，前章で定義した MTR の評価指標に address lifetime といった時間的な要素を付加し最大追跡可能時間 MTT(Maximum Tracking Time) といった値を定義する．これは第三者が特定のユーザを追跡し続けることのできる期間を直接的に評価関数として扱うものである．MTT の一例を図 16 に示す．第三者が無作為な時間 t_1 にユーザの追跡を開始し，ユーザは時刻 t_2, t_3, t_4 で silent period

を挟んでアドレスを更新している．例えば，第三者が t_2, t_3 の時に更新前後のアドレスを同一ユーザのものであると的確に判断でき， t_4 で初めてその判断を誤った場合を仮定すると，第三者はユーザの t_1 から t_4 までの移動軌跡の情報を取得可能であることとなる．この場合，MTT は t_1 から t_4 までの時間差分として計算される．

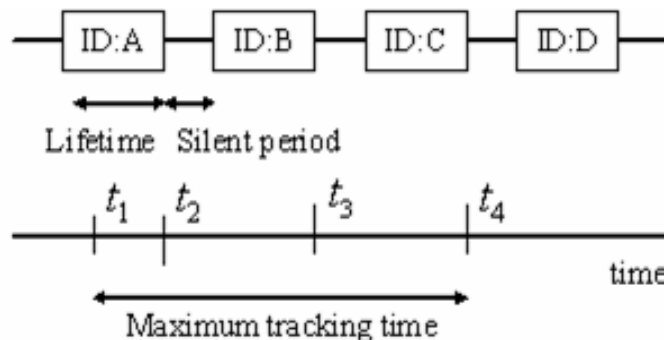


図 16: An example of Maximum Tracking Time

プライバシーの指標として MTT を定義したが，プライバシーと QoS のトレードオフの関係を解析するためには QoS に対しても指標を定義する必要がある．本研究では理論的な解析を明瞭に行うために主観的指標ではなく，客観的な数値指標を用いて QoS の指標とすることを考えた．ただし，先にも述べたように，使用するアプリケーションによって，考慮すべき点が異なる．まず，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には遅延が QoS の劣化に繋がるおおきな要因であるので，silent period の長さそのものが QoS の指標となる．一方，HTTP や FTP のようなノンリアルタイムアプリケーションでは，ユーザがデータ通信を要求する時間に通信可能なのか不可能なのかといったことが QoS に大きな影響を及ぼす．そこで，ここではノンリアルタイムアプリケーションの指標として通信不可能時間比 (CLR: Communication loss ratio) を定義する．これは通信不可能時間の占める比率であり，この値が小さいほど QoS は高いと考えられる．Silent cascade プロトコルにおいて CLR は address lifetime と silent period の比率であり，以下の式で表される．

$$CLR = \frac{\text{Silent period}}{\text{Address lifetime}} \quad (3)$$

以上，本節においては Silent cascade の適用を提案するとともに，プライバシーと QoS のトレードオフの関係を議論するための具体的な指標を定義した．

5.3 評価

本節において、シミュレーションおよび理論的な観点から Silent cascade によってもたらされる位置情報プライバシーの評価・解析を行う。

Silent cascade のプロトコル設計において考慮すべきパラメータは silent period の長さおよび address lifetime の長さである。これらの値を一定の QoS の確保を条件に、位置情報プライバシーへの効用を最大にするように設定する必要がある。我々はまず、いくつかの前提条件をおき、これら 2 つのパラメータおよびプライバシーレベルのメトリックである MTT の関係に関する理論式を求めることを行った。

ユーザが多段的にアドレスを更新していく中で、もし第三者が N 回の更新までこれらのアドレスを同一ユーザのものだと判断できた場合、これは第三者が $N \times T_l$ の時間だけユーザを追跡できたことを意味する。ただし Address lifetime を T_l とする。またこの N とは前述の MTR と同義である。これに加えて、第三者が追跡を始めてから、ユーザが最初にアドレスを更新するまでの時間も追跡時間には含まれると考えている。もし外部者が無作為に追跡を始めるとすると、 $T_l/2$ の時間が期待値としてこの時間に与えられる。以上の 2 点より MTT は MTR と Address lifetime(T_l) を用いて以下の式で与えられる。

$$E[MTT] = E[MTR] \times T_l + \frac{1}{2} \times T_l \quad (4)$$

一つの silent period のステージを超えて、第三者が追跡を続けることができる確率をここで p と定義する。言い換えれば、ユーザがアドレスを更新した際に、第三者が更新前後のアドレスを同一ユーザに属していると判断することに成功する確率である。Silent cascade において各ステージで p が不変であると仮定すると、 $(n-1)$ 回のアドレス更新の時点まで追跡に成功し、 n 回目のアドレス更新において追跡に失敗する場合の確率は以下の式で与えられる。

$$p^{n-1} \times (1 - p) \quad (5)$$

これに基づいて MTR の期待値は以下ようになる。ただし Silent cascade の段数は無限大であると仮定している。

$$E\{MTR\} = \sum_{n=1}^{\infty} (n-1) \cdot p^{n-1} \cdot (1-p) \quad (6)$$

ここで $p < 1$ であることを前提に近似式を用いると MTR は以下ようになる。

$$E\{MTR\} \doteq \frac{p}{1-p} \quad (7)$$

追跡の成功確率 p は第三者の追跡手法によって異なる. 3 章で **simple tracking**, **correlation tracking**, **Kaliman tracking** よ 3 つの手法を議論したが, ここではもっとも簡単な **simple tracking** を想定して理論式の導出を続ける. **simple tracking** は **GAS** に含まれる位置情報の中から無作為にターゲットのアドレスを選び出すという追跡手法のみを考える. この場合 p は **GAS** のサイズにのみ依存し, 以下の式で与えられる. ただし, ここでの **GAS** は **mixer** によって構成される **GAS** を意味している.

$$p = \frac{1}{1 + |\text{GAS}|} \quad (8)$$

mixer によって構成される **GAS** のサイズの理論値においては, 各ノードが同期してアドレスを更新し, また各ノードが連続的に通信を行っているという仮定の下, 以下の式で与えられる. なお, ノード (厳密には **mixer**) 密度 D , ユーザの移動速度 v , **Silent period** の長さ T_s とし, 測位誤差の影響は考慮していない.

$$|\text{GAS}| = D \cdot \pi \cdot (T_s \cdot v)^2 \quad (9)$$

以上, 式 (4)(7)(8)(9) より, **MTT** は以下の式となる.

$$E[\text{MTT}] = \frac{T_l}{D \cdot \pi \cdot (T_s \cdot v)^2} + \frac{T_l}{2} \quad (10)$$

また本稿においては理論値だけではなく, シミュレーションによる解析も行っている. これは理論式では考慮しきれなかった誤差モデルの影響などを評価・解析するためである. シミュレーションは 4 章でのシミュレーションと同様のものを用いた. ただしユーザは **silent cascade** の手法に従って多段的にアドレスを更新し, 評価関数としては **MTT** を用いている. シミュレーションにおける各パラメータの値を表 2 にまとめる

以下ではアプリケーションのタイプにわけてプライバシーおよび **QoS** のトレードオフの関係について解析を行っていく.

A. リアルタイムアプリケーション

リアルタイムアプリケーションの場合には **silent period** の長さを **QoS** の指標として扱うことができる. ここで式 (10) を $\text{lifetime}(T_l)$ の関数として考えると以下のようになる.

$$E[\text{MTT}(T_l)] = aT_l \quad \text{where} \quad a = \frac{1}{D \cdot \pi \cdot (T_s \cdot v)^2} + \frac{1}{2} \quad (11)$$

表 2: Simulation Configuration for Evaluating Silent cascade

Parameter	Value
Simulation Area	180m × 180m
Mobility model	Random waypoint (Speed = 0.5-1.5 m/s)
Init position of node	Uniform distribution
Traffic model	Periodic transmission or no consider
Tracking method	Simple tracking
Number of nodes	50-200
Positioning error	0.0-3.0m (Uniform distribution)
Silent period	100ms-1000ms in real-time application
Communication loss ratio	0.01-0.1 in Non real-time application
Address lifetime	100-1000s

QoS が一定である場合, a は正の定数となり lifetime が短いほど MTT は小さくなることが分かる. つまり一定の QoS レベルを維持しながらも, プライバシーレベルを最大にするためにはできる限り lifetime を短く設定することが効率的であるとの見解を得られる.

また Address lifetime を 200s に固定した場合の silent period と MTT の関係についてシミュレーションの結果を図 17 左に示す. 横軸が QoS の指標である silent period, 縦軸がプライバシーの指標である MTT となっており, ノード数 50, 100, 200 の各場合の結果を示している. 図 17 より Silent period が長くなることにより MTT が小さくなっていることがわかるが, これは QoS が劣化するにつれてプライバシーが向上するという明確なトレードオフの関係を示しているグラフといえる.

また silent period を 500ms で固定し, Address lifetime と MTT の関係を示したグラフが図 17 右である. これは一定の QoS を前提とした場合に, 短い lifetime がより高いプライバシーレベルを実現できることを示しており, 理論式から得た見解と一致する. ユーザがより頻繁にアドレスを更新することにより, プライバシーレベルは向上するといえる.

B. ノンリアルタイムアプリケーション

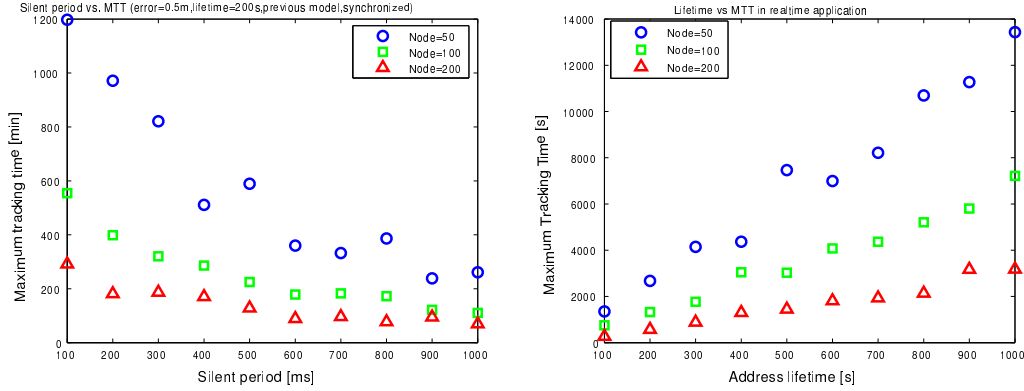


図 17: Evaluation in Real-time application

ノンリアルタイムアプリケーションの場合には，CLR を QoS の指標として考えることができる．式 (10) において CLR を c ，MTT を lifetime の関数として書き直すと以下ようになる．なお，silent period, lifetime, CLR の間の関係は式 (3) を用いている．

$$E[MTT(T_l)] = \frac{a}{T_l} + \frac{T_l}{2} \quad \text{where} \quad a = \frac{1}{D \cdot \pi \cdot (c \cdot v)^2} \quad (12)$$

ノード密度，CLR，そして移動速度が一定であれば，MTT は特定の T_l の値で極小値をとる形となる．極小値を与える L は

$$\frac{d(MTT)}{T_l} = 0 \quad (13)$$

の方程式により求めることができ，解は

$$T_l = \sqrt{\frac{2}{D\pi c^2 v^2}} \quad (14)$$

となる．一定の QoS を前提とした中で，最小の MTT，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の見解を得る．

図 18 左に lifetime を 200s に固定し，CLR と MTT の関係を示したシミュレーションの結果を示す．CLR が大きいほど MTT が小さくなっていることが分かるが，これは図 17 と同様に QoS とプライバシーのトレードオフの関係を明確に示している結果といえる．

さらに図 18 右においては，QoS の指標である CLR を固定した中での，lifetime

と MTT の関係を示したグラフを示している．ノード数を 50,100,200 とし，ここで測位誤差の影響は考慮していない．このグラフをみると，まず上記の理論式とシミュレーションの結果がよく合致していることがわかる．またその解析に従って，MTT を最小とする最適な lifetime が存在していることがわかる．

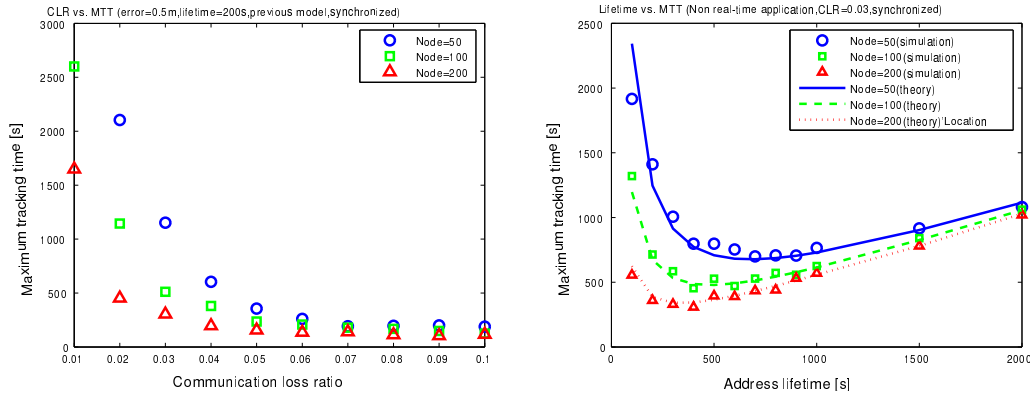


図 18: Evaluation in Non Real-time application

5.4 考察

本節においては，理論式で解析しきれなかった通信トラフィック，測位後差の影響に関する考察および実際の都市空間における Silent cascade の設計指針についての考察を行う．

前節で論じた理論式の導出においては，測位誤差を考慮せず，また通信トラフィックは連続的に発生しているものと仮定していた．しかしながら実際にはこれらの要素もユーザの位置情報プライバシーに少なからず影響を及ぼすものといえる．4章での解析にもとづくと，測位誤差が大きいほど，そして通信パケットの発生する間隔が長いほど，GAS に含まれる位置情報が大きくなることがわかっている．図 19 においては，そのような理論式に対して，測位誤差および通信トラフィックを考慮した場合のシミュレーション結果との比較を示す．図左が測位誤差，図右がトラフィックの影響である．まず誤差に関してしてみると，高精度の測位が行われる場合には理論式に近い傾向がみられるが，精度が低いような場合には，lifetime が最適値よりも小さい場合でも短い MTT が実現されている．理論式および高精度の測位の場合，lifetime が最適値より短い場合，CLR 一定の中では silent period の長さが短く，十分な GAS を確保できないために MTT の増加につながっていた．しか

しながら、誤差の大きな場合、ある程度 **silent period** が小さくても、誤差の影響により **GAS** に含まれるノードが多くなり、プライバシーの確保がされと考えられる。同様なことは通信トラフィックに関してもいえる。通信トラフィックの送信間隔が小さい場合は理論式に近い傾向がみられるが、送信間隔が大きくなると **silent period** が小さな場合でも十分なプライバシーレベルが確保されている。

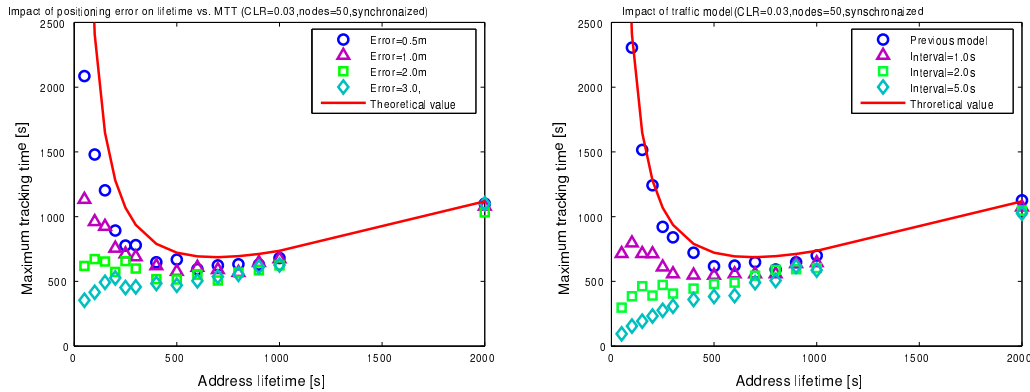


図 19: Impact of positioning error and traffic interval

式(14)に基づくと,CLR一定のもとで最高のプライバシーレベルを実現する **lifetime** の値はノード密度に依存するといえる。図 20 左には理論式に基づいた最適な **lifetime** とノード密度との関係をグラフ化した。それぞれの線は CLR の異なる値を示している, 図 20 よりノード密度が大きいほど最適な **lifetime** が小さいことがわかる。このことは図 18 の結果とも合致している。CLR 一定のもとでは **lifetime** が大きくなると, **silent period** の値も大きくなるが, ノード密度が大きな場合には, そのように長い **silent period** を必要とせず, 十分な **GAS** を確保できる。従って, 長い **lifetime** は, アドレスを変換するまでの時間を長くし結果として追跡される時間を長くするといったマイナスの効果のみをもつこととなる。このように考えるとノード密度が大きい場合ほど, 長い **lifetime** は必要なく, 最適な **lifetime** は小さいものとなると考えられる。

このように最適な **lifetime** はノード密度に依存するといえるのだが, 実際に **Silent cascade** を設計し, 都市空間で利用することを考えると, ユーザの所属する環境のノード密度は時々刻々と変化するものである。ユーザの移動に伴って環境が変化する場合もあるし, たとえユーザが同一の環境に留まっていたとしても時間とともにその場のノード密度は変化する。このようなことを考えると **lifetime** の値を固定値とすることは難しく, 我々は環境に合わせて動的に変化する可変の **Lifetime**

が必要であると考えている。無線 LAN のシステムを考えるとこの環境に合わせて **lifetime** の値の調整は各ユーザが属するエリアのアクセスポイントが行うことができると考えられる。図 20 右には理論式にもとづくものであるが、固定の **lifetime** の場合と各ノード密度にあわせて最適な **lifetime** を設定した場合との比較を示す。固定の **lifetime** の場合、たとえば短い 500s に固定すると、ノード密度が大きいような場合には短い **MTT** を実現できるが、ノード密度が小さいような場合に **MTT** が非常に大きくなってしまう。逆に 2000s といった長い **lifetime** で固定した場合には、ノード密度が小さい場合には有効に機能するが、ノード密度が大きい場合に **MTT** が大きくなってしまう。このような中で動的に **lifetime** を変化させた場合は、どのノード密度においても小さな **MTT** を実現可能であり、ユーザが所属する環境の変化に対応可能であると考えられる。ただし、今回は理論式にもとづいた上での評価であるため、実際にはノード密度の変化をどの程度の間隔で測定し、**lifetime** を変更するのかなどといったより詳細な考察が必要となる。

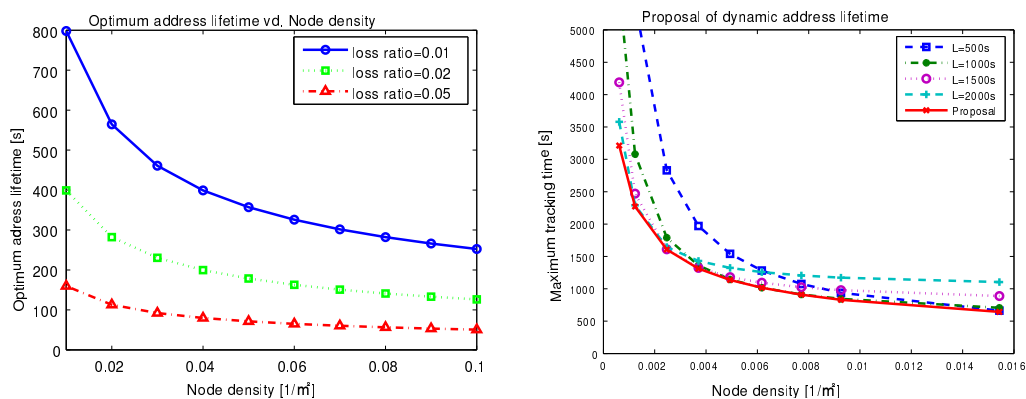


図 20: Optimum address lifetime

6 RFID への応用

Silent period の手法は無線通信端末の分野にのみ有効な位置情報プライバシー保護手法ではなく、そのシンプルな機構ゆえに他の様々な分野に応用可能であると考えている。その一つのケースとして本論文においては RFID システムの分野を取り上げる。近年、大きな注目をうけている RFID システムであるが、そのセキュリティの問題の一つとしてタグを所有するユーザが長時間にわたって追跡されてしまうといった位置情報プライバシーの問題が指摘されている。本章においては RFID における追跡問題に対し、Silent period の手法を応用していくことを考える。

6.1 背景

現在、世界中で様々な自動認識システムが使用されている。自動認識 (Automatic Identification) とは、「人間を介さず、ハード、ソフトを含む機器により自動的に内容を認識する」ことである。欧米では同義語として AIDC (Automatic Identification and Data Capture) も、使用するようになってきている。自動認識技術としてはバーコード、磁気カード、OCR (Optical Character Recognition) などがあるが、このような自動認識システムの一つとして近年、大きな注目を集めている技術が無線通信を利用した自動認識技術である RFID (Radio Frequency Identification) である [35]。流通分野においてはバーコードに変わる商品識別手法としてあらゆる商品に電子タグを取り付けるといった動きがある。これは EPC (Electronic Product Code) などと呼ばれるが、バーコードと比べて無線通信を利用した RFID システムは無線通信を利用しているため、複数の商品を非接触で識別するといったメリットがあり、流通の効率化が図られるものとされている。製品に ID 情報を割り当てるための規格制定では米マサチューセッツ工科大学 (MIT) が中心となって進めている「EPCglobal[31]」(前身「Auto-ID Center」) の取り組みが先行しており、Wal-Mart Stores 社など多くの大手流通業者なども参加している。また流通分野だけではなく、RFID はそのアプリケーションの幅を広げようとしている。たとえば商品に取り付けられた電子タグと家庭の家電が連携して消費者にサービスを提供するといった情報家電の開発が進められている。また公共交通機関での運賃支払いシステムにも RFID が使われており、日本でも 2001 年 11 月から JR 東日本が Suica (Super Urban Intelligent Card) のサービスを開始され、今では利用が一般的になってきた。このような RFID の普及をうけて、我々が常に RFID のタグを持ち歩くような環境

表 3: Classification of RFID tag

Class	Memory	Power source	Features
0	None	Passive	Article Surveillance
1	Read-only	Any	Identification only
2	Read-Write	Any	Data logging
3	Read-Write	Semi-passive/Active	Environmental sensors
4	Read-Write	Active	Ad Hoc Networking

は近いと考えられる。

RFID システムは ID を割り当てられたタグ、タグの発する無線信号を読み取るためのリーダーそしてタグの ID 情報を管理するデータベースによって動作する。RFID タグは、ラベル型、コイン型、カード型など用途に応じて様々な形状があり、また電源方式によってアクティブタグとパッシブタグに分けられる。アクティブタグは、RFID タグ内に電池が内臓されており、自ら電波を発するものである。パッシブタグは、アンテナでリーダーからの電波を受信することで起動電力を得るものである。またアクセス方式にも Read Only 型、Read Write 型などがあり、これらのタグは用途によって分類される。表 3 には Auto-ID センターが定めた RFID タグの分類を示す。EPC サービスのために一般的にクラス 2 のパッシブタグの仕様が想定されている [37]。

RFID システムの動作の概要を図 21 に示す。まずリーダーがタグに対して呼びかけ（クエリー）を行う。タグはそのクエリーに対して自身の ID あるいはそれに代わる信号を返答する。リーダーはタグから返信された情報をデータベースに送ることで、そのタグに関する情報を得る。ここでは一般的にリーダーとデータベース間の通信はセキュアなものであると仮定されることが多い。なぜならその部分の通信は有線でも可能であるし、またリーダー、データベースともに十分なリソースを確保できるためにセキュアな通信環境を実装可能であるからである。それに対してタグとリーダー間の通信は無防備であるといわれる。これはタグがコスト・サイズなどの強い制約がかかり、複雑の防衛機構を組み込めないためである。なお、リーダーからタグへの問いかけの通信を Forward Channel、タグからリーダーへの通信を Backward Channel といって区別することが多い。前者は通信半径が 100m 程度と長い場合が多いが、後者はタグの種類にもよるがせいぜい数 m 程度の場合が多い。

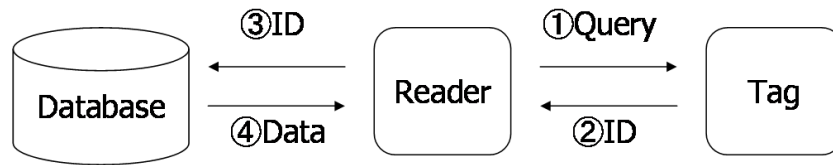


図 21: RFID system

RFIDによって多くの有用なアプリケーションが実現される一方、RFIDシステムにおけるセキュリティ面では様々な問題も指摘されている。これは先ほども指摘したようなタグとリーダー間の無線通信の無防備さが原因となっていることが多い。基本的にタグはリーダーからのクエリーに対して自身のIDを返答するだけのシンプルな設計がされているため、RFIDリーダーさえあれば、第三者でも不当にタグのIDを読み取ることができる。またリーダーとタグ間の通信は無線を介して行われるため、タグを所有する消費者が気づかないうちに情報を読み取られるといったことが懸念される。米国ではセキュリティ面への不安から、タグをつけられた商品の不買行動も起こっており、RFIDのセキュリティは重要な課題となっている。

セキュリティ問題は無線通信端末の場合と同様にデータプライバシーと位置情報プライバシーの大きく2つに分けられる。前者は商品に取り付けられたタグの発する信号がIDだけでなく商品に関する情報なども含んでいる場合があり、そのような時に第三者が電波を傍受するとその人の所有物など情報が漏れてしまうことである。このような問題は基本的にタグがIDそのものを応答する代わりにPIDを応答することによって解決される。PIDは何らかの手法によりID情報を暗号化したものである。代表的な手法にHash-Lockingといったものがある[37]。図22に示すように、この手法においてはIDをハッシュ関数にかけ、それによって生成したものを応答するPIDとして扱う。データベースで復号してID情報を得ることができる。ただしこのような手法ではデータプライバシーは守れても位置情報プライバシーは守ることができないとされる。PIDが固定である以上、それがなにを意味しているのか分からなくても、そのPIDを追跡することでそのタグをもつユーザの位置情報の履歴を得ることが可能となるからである。この際の位置情報の識別子はタグのPIDであるが、2.2節で論じたように、長時間追跡されることで十分にユーザそのもののプライバシーを侵害し得る。このような問題の本質はタグが固定のPIDを応答し続ける点にあり、近年の論文では可変のPIDを返答することを提案されている。本章においては、このようなPIDを用いた場合を前提とし、時間的・空間的相関を利用して追跡されてしまう問題点に着目し、silent periodをRFIDプライバ

シーに応用することを提案し, その評価を行う.

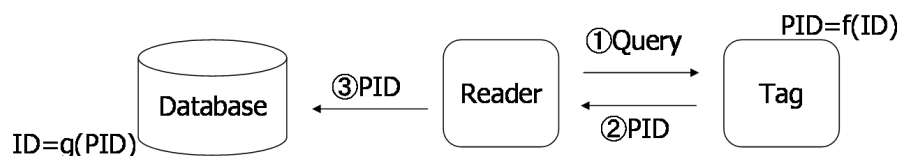


図 22: Hash Locking

6.2 想定環境

本論文で想定している RFID システムの概要を図 23 に示す. システムの主な構成要素はタグを所有するユーザ, ユーザのタグを認証可能なサービスプロバイダーおよびユーザの位置情報プライバシーを侵害し得る攻撃者の 3 つである.

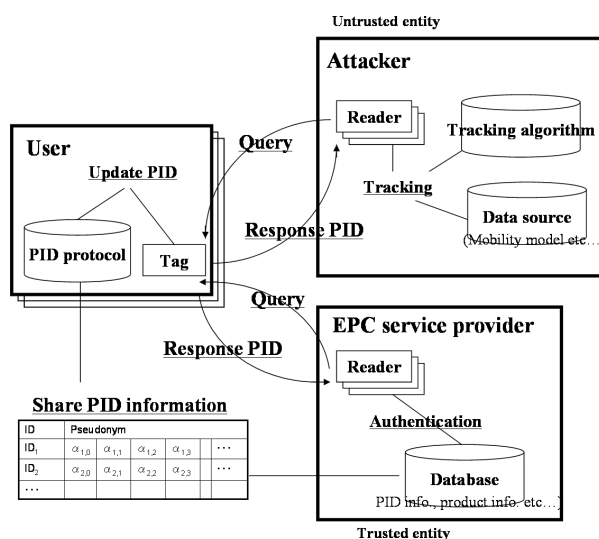


図 23: RFID system model

ユーザは RFID タグが付与された商品を保持することで, タグの所有者となる. このタグはリーダーからのクエリーに対して自身の ID に代わる PID を応答する. タグの中には特定のリーダーにのみ応答するタイプもあるが, 本論文においてはすべてのリーダーに対して同様に応答するものと仮定している. 第三者による長時間の追跡を避けるためにタグの PID は定期的に更新される必要がある. 先行研究としては Minimalist cryptography[33] や Hash Chain[34] などの手法がある.

Minimalist cryptography は可変の PID を生成するもっともシンプルな手法であ

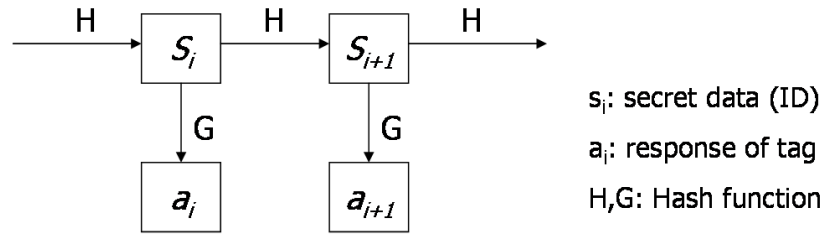


図 24: Hash Chain method

り、予め一つのタグに対して複数の PID を割りあてておく手法である。そしてリーダーからのクエリーごとにこの PID を順々に応答していくことで、応答される各 PID が可変のものとなる。

一方、Hash Chain 方式の場合は、PID を生成するために多段的にハッシュ関数を利用している。図 24 のように元となる s_0 にハッシュ関数 H を用いて s_1 を生成する。リーダーからクエリーがあった場合にはこの s_1 を別のハッシュ関数 G を用いて暗号化した a_1 を応答するとともに、ID 情報の s_1 をさらにハッシュ関数 H を用いて s_2 へと更新する。このようにすることで次回にクエリーがある際には s_2 をハッシュ関数 G で暗号化した a_2 を応答することが可能で、可変の PID が実現される。

次にユーザに種々のサービスを提供するプロバイダーであるが、サービスを提供するためには、クエリーに対して返ってきた PID から、そのユーザの真の ID 情報を認証しなければならない。このために PID 情報をタグと共有しているデータベースにアクセスする必要がある。例えば Minimalist cryptography の手法の場合、共有される PID 情報はタグの固定の ID とそれに割り当てられた複数の PID の対応リストとなる。そのリストの中から、タグから応答された PID を検索することによって、その PID に対応する真の ID 情報を引き出すことができる。一般的に管理するタグの数 n 、一つのタグに割り当てる PID の数 m である場合、 $n \times m$ の全探索が必要となる。また Hash Chain 方式の場合には元となる ID 情報 s_0 とハッシュ関数 H, G を共有して管理しておくことによって同様に探索し、応答される信号から ID 情報を復号化できる。

最後に攻撃者であるが、これは上記のデータベースにはアクセスすることはできないが、リーダーを所有することでタグの PID を盗聴することができる。攻撃者は複数のリーダーを都市環境中に配置し、タグを所有するユーザがこれらのリーダーの近く（タグの通信半径内）を通る場合にリーダーはタグの PID を取得できる。さらにそのクエリーかけた時間、そのリーダーの配置してある場所の情報から、

識別子 id , 場所 s , 時刻 t からなるユーザの位置情報データ (id, s, t) を取得することが可能である。ただし、ユーザが応答する PID が頻繁に更新される場合、各 id の位置情報データの集合は短い移動履歴となるが、攻撃者は時間的・空間的な相関を利用して複数の id の位置情報を結合させ、特定のユーザを長時間にわたって追跡することができる。

図 25 には RFID システムにおける時間的・空間的相関の一例を示す。タグを所有したユーザが通路に沿って移動していき、通路沿いに置かれた RFID リーダーによって連続的に PID を測位されている。PID 自身は測位ごとに異なるものの、それぞれの PID が測位される時刻・場所は一貫した連続性があり、攻撃者にとってみればユーザの移動軌跡を推測することが可能となる。

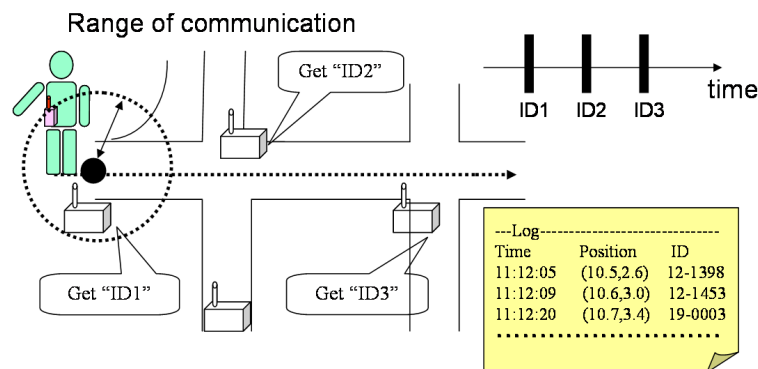


図 25: Attack model in RFID system

時間的・空間的相関を利用した追跡問題に関しては RFID システム分野以外には先行研究で述べた位置情報サービスあるいは我々が考察した無線通信端末（無線 LAN, Bluetooth）といった分野で議論されている。これらの分野と比較して今回の RFID システムにおける位置情報プライバシーの場合には以下のような特徴が挙げられる。

一つは測位可能のエリアの制限である。位置情報サービスの分野で使われることの多い GPS や WLAN, Bluetooth といった無線通信端末の場合、たとえ建築物などの障害物の影響で位置推定精度が落ちるとしても、サービスエリアの全体でユーザの位置を推測することができると想定される。つまりこれらのデバイスの場合、空間的に測位可能エリアの制限がないといえるのだが、RFID 測位の場合にはリーダーの近傍をユーザが通過した場合にのみユーザの位置を取得可能である。これは赤外線などとも共通するものであり、2 章で述べた近接検知方式の測位手法である。RFID 測位の場合の近傍とは具体的にはタグの通信半径に依存し、それはせいぜい

数 m 程度である。したがって攻撃者がユーザの移動するエリア全体を測位可能であるといった状況は考えにくく、攻撃者にとって測位可能エリアが制限されている環境であるといえる。

また攻撃者が得られる位置情報の質といった点に目を向けると、RFID の測位の場合、タグの通信半径に依存した位置情報の粒度をもつこととなる。たとえば、タグの通信半径を r とし、ある点 (x, y) に配置したリーダーがユーザの PID を観測した場合、攻撃者が得られる情報は「PID のタグをもつユーザが点 (x, y) を中心とした半径 r 内のどこかに存在している」といった曖昧さを含んだ位置情報になる。

また、PID を更新するタイミングを考えてみると位置情報サービスあるいは無線 LAN の場合には各ノードが同期して PID を更新することが可能である。位置情報サービスの場合にはミドルウェアが、無線 LAN の場合にはアクセスポイントが各ノードの更新タイミングを調節することが可能であるためである。それに対して RFID の場合を考えてみると、タグはリーダーからの電力供給をうけて動作する仕組みのため、各ユーザが所有するタグ同士が協調して PID の更新を行うとは考えにくく、それぞれのタグが非同期で PID を更新することが想定される。このような場合、あるユーザを追跡しようとしている攻撃者にとって、そのユーザが PID を更新する時間帯とまったく異なる時間帯で PID を更新しているような他ユーザは無視することができるため、より追跡しやすい環境といえる。

6.3 RFID におけるプライバシー保護手法

本論文においては、我々が無線通信端末のプライバシー保護のために考案した 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のために応用することを提案する。タグがリーダーからのクエリーに応答しない期間 silent period を設けることにより PID 更新前後の位置情報の時間的・空間的相関を小さくし、攻撃者にとってみれば特定のユーザを追跡することが困難になると考えている。

具体的な手法であるが、まず基本的に RFID タグはリーダーからのクエリーがあるたびに自身の PID を応答するとともに、自身の PID を更新する。PID 更新の手法に関しては 2 章において述べたとおりである。ここではすべてのクエリーごとに PID を更新するような場合と、時々更新するような場合との両方が考えられる。ここではクエリーごとに一定の確率（PID 更新確率）で PID を更新するとしてモデル化する。

PID を更新した場合、一定の silent period を設ける. Silent period の期間はたとえリーダーからクエリーをかけられても PID を応答しない. つまり攻撃者の立場からすればこの期間はタグを測位することができない期間である. 図 26 に RFID システムにおける silent period の図を示す. ユーザ 1 は PID:A を応答した後に silent period に入り, silent period の期間が終わった後に PID:A' をリーダーに測位されている. 同様にユーザ 2 は PID:B から PID:B' へと PID を更新している. ここで二人のユーザが silent period に入っている間はリーダーは測位できない. そのため図の中央にあるようなリーダーはたとえユーザがその近傍を通過したとしても PID 情報を得ることが出来ない. このことで特定のユーザ, たとえばユーザ 1 を追跡しようとしている攻撃者にとってはユーザ 1 の新しい PID が A' なのか B' なのかの判断がより困難になると考えられる.

さらに今回の RFID システムの場合, 非同期に PID を更新するといった特徴がある. このような場合, 固定長の silent period では更新前後の PID で測位される時間的關係が推測されやすく, それを利用して追跡されるおそれがある. このような時間的相関を利用したアタックに対してここでは silent period を可変長にすることを提案する. silent period の平均長 l とし, その中のある比率 q の長さを可変部分とする場合, $l \times (1 - q)$ と $l \times (1 + q)$ の間を一樣分布する値の長さとなる.

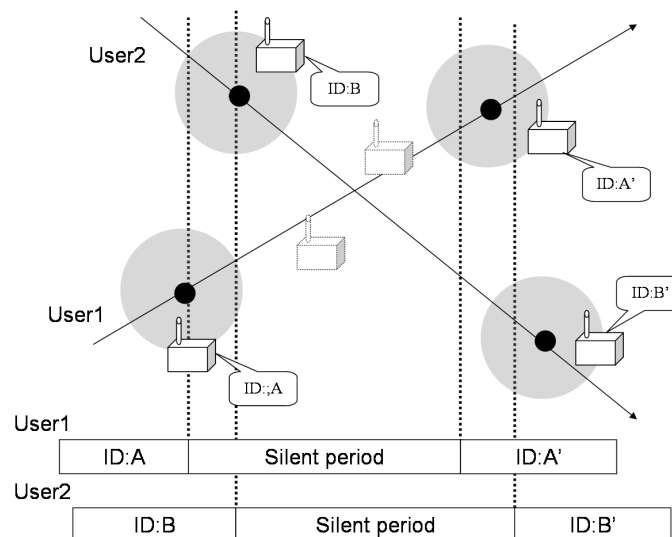


図 26: Illustration of silent period in RFID system

6.4 評価

タグを所有した各ユーザが、タグのPIDを連続的に更新しながら複数のリーダーが配置された一定のエリア内を移動している環境を想定しシミュレーションを行った。

ユーザの移動モデルに関してはエリア内のすべてを自由に動き回る場合と、都市空間の通路あるいは道路といったような動ける範囲に制約がある場合とを評価した。前者に関してはRandom waypointモデルを、後者に関してはManhattanモデルを利用した。今回はシミュレーションエリア100m四方、ユーザ数50とし、後者の移動モデルの場合、道路は垂直・水平方向に10m間隔で配置されたものを想定した。また後者の移動モデル場合、各交差点で方向を変える確率は右折、左折ともに25

攻撃者に関してはエリア内に一定数のRFIDリーダーを配置することでユーザを追跡する。リーダーは垂直・水平方向に一定間隔で配置するものとして、Manhattanモデルの場合は、各交差点にリーダーを配置するモデルとなる。リーダーはタグの通信半径内にまでユーザが近づいた場合にユーザの位置情報を取得する。なお、実際には環境によりこの通信半径にばらつきが生じていたり、あるいはたとえ通信半径内タグが近づいたとしても認識することができないといったことも考えられるが、今回はそのような点は考慮していない。つまりタグの通信半径にリーダーが存在している場合、攻撃者は必ずそのユーザの位置情報を取得できるということである。シミュレーションではリーダーの数、およびタグの通信半径をパラメータとして変化させ評価を行った。

プライバシー保護機構に関しては、前節でも述べたPID更新確率 p といったパラメータを設けた。これはPIDの更新頻度を決定する要素となり、 $p = 1.0$ ならばすべてのクエリーごとにPIDを更新するようなことを意味する。またPIDを更新した場合には固定長あるいは可変長のsilent periodを設けることとした。PID更新確率およびsilent periodの長さ、可変とする部分の比率(variable ratio)が評価パラメータとなる。

シミュレーション環境の主なパラメータを表4にまとめる。なお、評価指標としてはGASのサイズを用いた。

まずsilent periodを設けない場合の評価を行った。図27にはManhattanモデルでPID更新確率を変化させた場合の結果を示す。これをみると更新確率が高いほどGASのサイズが大きくなることがわかる。これは、PID更新確率が高いとターゲット

表 4: Simulation Configuration for RFID systems

Parameter	Value
Simulation Area	100m × 100m
Mobility model	Random waypoint or Manhattan mobility speed=0.5-1.5 [m/s]
Init position of node	Uniform distribution
Communication of tags	1.0-3.0 [m]
Number of nodes	20-100
PID update probability	0.2-1.0
Silent period	0.0-5.0s (variable ratio: 0.0-1.0)

トの位置情報と時間的にオーバーラップするほかの位置情報の数が増えるためだと考えられる. また各線はエリア内を移動するユーザ数の各場合を示しているが, ユーザ数が多いほど **GAS** のサイズが大きくなり匿名性が向上することもわかる.

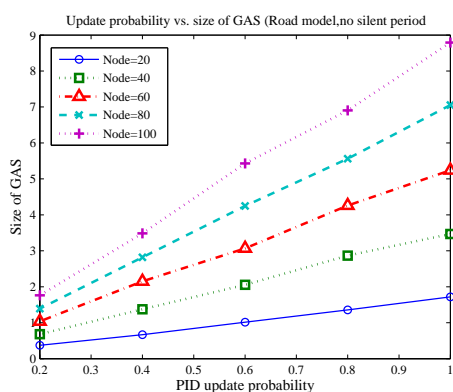


図 27: Impact of PID update probability

次に, タグの通信半径の影響を評価するために Random waypoint モデルにおける評価を行った. 通信半径が **RFID** 位置情報プライバシーにもたらす影響は2つあると考えられる. 一つはタグの通信半径が大きいほど攻撃者が測位可能なエリアが大きくなる点である. このことによってユーザはより頻繁に測位され追跡されやすくなると考えられる. 測位可能エリア (coverage) はリーダーの数を N , タグの通

信半径を r ，全体のエリア面積を S として以下の式で与えられる。

$$Coverage = \frac{N \times \pi \times r^2}{S}$$

もう一方は攻撃者の得られる位置情報の粒度がタグの通信半径に依存する点である。通信半径が大きくなることで粒度が荒くなり，攻撃者にとってみれば追跡がより困難になると考えられる。

図 28 左はタグの通信半径を横軸に，縦軸に **GAS** のサイズをプロットした。リーダ数は一定である。これをみると通信半径が大きいほど **GAS** が小さくなっているが，これは測位可能エリアが大きくなることで測位間隔が小さくなるためだと考えられる。つまり通信半径がもつ 2 つの影響のうち位置情報粒度の影響よりは測位可能エリアの影響が支配的に働いているといえる。一方，図 28 右は測位可能エリアを一定にしたままでタグの通信半径の影響をみた。この場合，測位エリアの影響は無視できるため，位置情報粒度の影響により通信半径が大きいほど **GAS** が大きくなっていることが分かる。

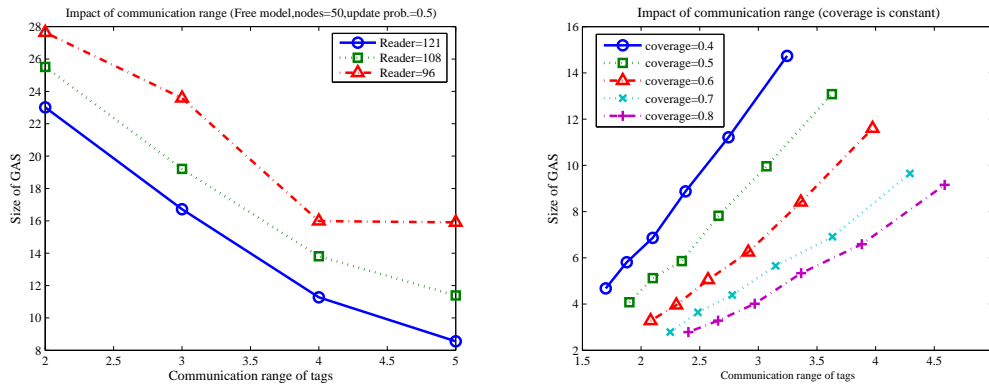


図 28: Impact of communication range of tags

つぎに我々の提案している **silent period** を設けた場合の評価結果を図 29 左に示す。この図より，より長い **silent period** を設けることにより大きな **GAS** を確保することができることがわかり，**silent period** によって位置情報プライバシーが向上していることがわかる。また図 27 の結果と同様に **ID** 更新確率が高いほど **GAS** が大きくなることも読み取ることができる。

ここで **ID** 更新確率について考えてみるとプライバシー保護のためにはより頻繁に **ID** を更新することが望まれるが，更新確率が高くなると，その分，一つのタグに割り当てべきアドレス空間が大きくなると考えられる。このことはデータベー

ス側でタグの認証を行う際の計算コストの増大につながり、システムを運用する観点からは高い更新確率は望ましくないのではないかと考えている.たとえば n 個のタグを管理するシステムにおいて,一つのタグに対して m 個の PID を割り当てなければならない場合,認証する際には $n \times m$ の全探索の計算が必要となる.このような点を考えたとき,低い更新確率でも **silent period** を設けることにより,高い更新確率と同様のプライバシーレベルを実現できることは一つの利点であると考えられる.例えば図 29 左をみると,更新確率が 1.0 で **silent period** を設けない場合の GAS サイズはおよそ 4 であるが,更新確率を 0.6 としても **silent period** を 10s 程度設ければ,それと同様なプライバシーレベルが実現される.**Silent period** は位置情報プライバシーを向上させるとともに,このように認証コストを抑制したい場合にも **silent period** は貢献できると考えられる.図 29 右においては一定のプライバシーレベルを実現するための更新確率と **silent period** の長さの関係をグラフ化している.一定のプライバシーレベルを実現させるためには長い **silent period** を設ける,更新確率を高くするの 2 つの戦略があるといえる.

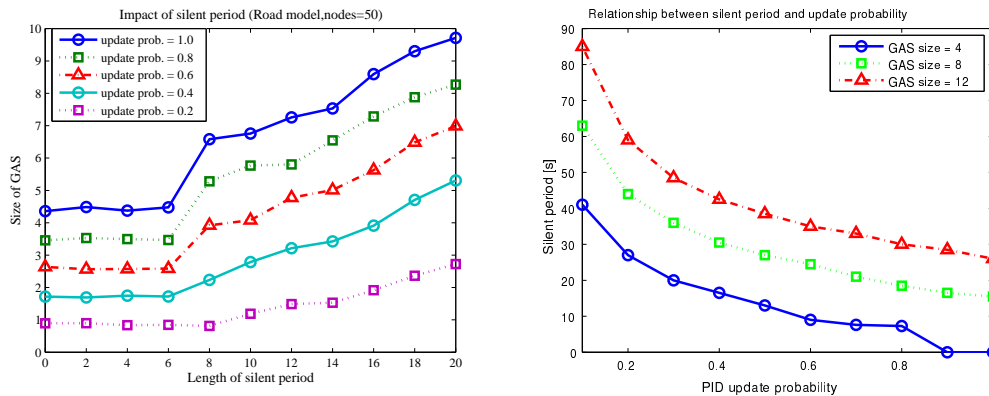


図 29: Impact of silent period in RFID system

最後に **silent period** を固定長でなく可変長にした場合の評価を行った.RFID システムの場合, PID の更新が各ユーザ間で非同期で行われるため同期の場合に比べてターゲットの位置情報と時間的に相関をもつユーザが少なくなる.このような中で可変長の **silent period** を設けた場合, ターゲットの位置情報が測位されてから次に測位されるまでの時間帯が曖昧になるため, より多くのユーザがこの時間帯に測位されることになる,つまり時間的に相関をもつと考えている.図 30 左には,そのことを視覚的に示すためにターゲットの **silent period** を挟んだ 2 つの位置情報の時間差分 Δt の値のヒストグラムを示す.可変の **silent period** の割合が大きくなる

につれてその分布が広がっていることがわかる. このことは **GAS** を計算する際のパラメータである **Detection window(D_w)** が大きな値になることにつながる. このような影響をうけて時間的に相関をもつ位置情報が増加し, **GAS** のサイズは大きくなると考えられる. 図 30 右には silent period と **GAS** の関係のグラフの中で可変長にした割合 (variable ratio) の影響を示している. Silent period を可変長にすることで **GAS** のサイズが大きくなり, より効率的に位置情報プライバシー保護が可能となると考えられる.

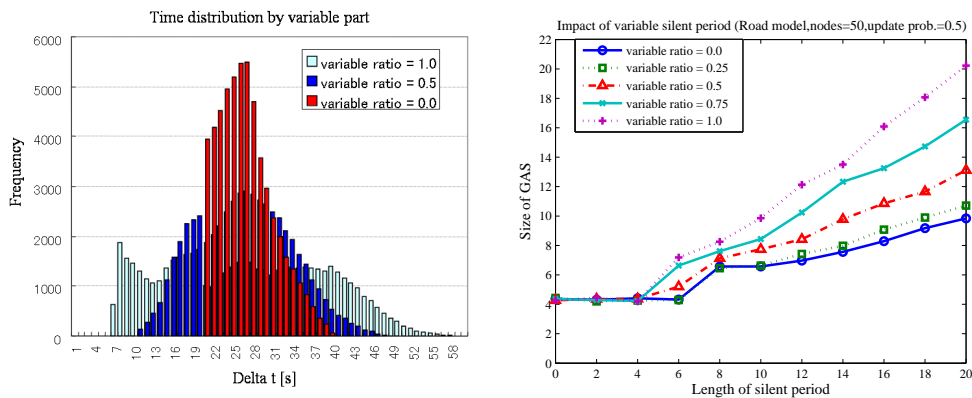


図 30: Impact of silent period in RFID system

7 結論

本論文においてはユビキタス情報環境における個人の位置情報プライバシーに関する議論を行った. ユビキタス情報環境においてはさまざまな有用なサービスを実現する位置情報であるが, 無線通信端末や RFID などの分野で個人の位置情報の履歴を個人の意図と関係なく第三者に取得されるといった危険性が存在している.

我々はまず位置情報の識別子を更新することによって長時間の追跡を回避するといった考えが, 高精度・高頻度の測位環境においては十分ではないということを指摘した. 識別子更新前後の位置情報の間に何らかの相関が存在しており, 第三者はその相関を利用して再び追跡を続けることができるためである. 本論文においては特に位置情報における時間的・空間的な相関を利用した追跡問題に着目し議論を進めた. そのような追跡を行う攻撃者モデルを想定し, 具体的な追跡手法に関して考察を行った.

識別子の更新前後における位置情報の非結合性を高め, 個人の位置情報プライバシーを保護する手法として我々は **silent period** と呼ぶ手法を提案した. **Silent period** とは識別子更新時におけるいっさい通信を行わない期間と定義される. この期間は攻撃者は個人の位置情報を取得することができず, 更新前後の位置情報の時間的・空間的相関は小さくなる. 結果として攻撃者が特定の個人を追跡することが困難になり, 個人の位置情報プライバシーのレベルは向上すると考えられる. さらに我々はこの **silent period** の有効性を示すにあたって, 位置情報プライバシーという概念的なものを定量的に評価するための手法として **GAS** の概念を提案した. **GAS** とは匿名通信におけるアノニミティセットの概念を応用したものであり, 「ある位置情報と時間的・空間的に相関のある位置情報の集合」と定義される. このような **GAS** のサイズ/エントロピーおよび攻撃者に用いる追跡手法の分析に基づく追跡時間といった定量的指標を用いて評価を行った結果, **silent period** の有効性を示すことができた.

より長い **silent period** を設けることにより個人の位置情報プライバシーレベルは向上するといえるが, 一方で **silent period** はサービス品質 (QoS) の劣化を招く. プライバシーと QoS とはトレードオフの関係にあるといえるが, 我々は個人の位置情報プライバシーと個人の使用するサービス品質との両立を図るべく **silent cascade** と呼ぶ手法を提案した. この手法の中でプライバシーと QoS との関係を解析し, ある一定の 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** の設計指針を得た.

最後に我々は **silent period** の手法を RFID システムにおける位置情報プライバ

シーの問題に応用することを考えた.RFID システムにおける位置情報プライバシーの問題を解析した結果,測位形式,攻撃者の得る位置情報の形式,そして識別子更新の同期制御といった3点に特徴があることがわかった.特に非同期の識別子更新といった特徴に着目し,silent period の長さを可変長とすることを提案した.非同期に識別子更新においては特定の位置情報と時間的に相関のある位置情報が減少してしまうのだが,silent period 可変長にすることで時間的に相関のある位置情報の数を確保することができる.このような RFID システムにおける silent period の手法を評価し,その有効性を示すとともに,本手法を用いることで位置情報プライバシーを保障しながらも RFID システムにおける認証コストを削減することができるのではないかといった見解を得た.

今後の課題としてはまずより実世界に近い環境での位置情報プライバシーの評価を行う必要があると考えている.そのためには実際の歩行者の移動軌跡の情報 [7],あるいは都市空間における道路・通路といった GIS データを利用していくことが有用であると考えている.また無線通信分野においては実環境においていかに最適な silent cascade のパラメータを動的に制御していくのかについて,RFID システムの分野においてはプライバシーレベルと認証コストの関係についてのより詳細な議論が必要だと考えている.

謝辞

本研究を進めるにあたり,非常に忙しい御身であるにも関わらず,研究その他の御指導して頂いた瀬崎薫助教授に心から御礼申し上げます.

常日頃より相談に応じていただき,多くの御助言を頂きました同研究室博士課程の黄楽平氏に感謝いたします.他研究室ながら有益な御助言を頂きました松浦幹太助教授,鈴木雅貴氏に感謝いたします.研究生活において様々なサポートをして頂いた小松邦紀助手,松本夏穂さんをはじめ研究室の皆様感謝いたします.

最後に6年間という本当に長い間,有意義な学生生活をさせてくれた自分の両親に感謝を表し,これを謝辞とさせていただきたいと思います.

平成18年1月31日

山根 弘

参考文献

- [1] Mark Weiser, “The computer for the 21st century,” Scientific American, 265(3):94-104, Sep., 1991
- [2] Anind K. Dey, Gregory D. Abowd, “Towards a better understanding of context and context-awareness”, Proceedings of the CHI 2000 Workshop on inThe What, Who, Where, When, Why and How of Context-Awareness11, 2000
- [3] P. Bahl and V. Padmanabhan, “Radar: an in-building rf-based user location and tracking system,” in Proc. of IEEE INFOCOM 2000, Tel-Aviv, Israel, 2000.
- [4] Hitachi, “Hitachi’s Air location,” 2004, <http://www.hitachi.co.jp/airlocation/>.
- [5] Udana Bandara, Mikio Hasegawa, Masugi Inoue, Hiroyuki Morikawa, “Design & Implementation of a Bluetooth Based Indoor, Location-sensing System”, Technical Report at the 3rd meeting of IPSJ Ubiquitous Computing System WG, Tokyo, Feb. 2004
- [6] I. Guvenc, C. T. Abdallah, R. Jordan, and O. Dedeoglu, “Enhancements to RSS based indoor tracking systems using kalman filter,” in Proc. of Intl. Signal Processing Conf. (ISPC), Dallas, TX, U.S., 2003.
- [7] H. Zhao and R. Shibasaki, “A novel system for tracking pedestrians using multiple single-row laser-range scanners,” IEEE Transactions on Systems, Man and Cybernetics Part A: Systems and Humans, vol. 35, no. 2, pp. 283-291, 2005.
- [8] KDDI, “EZ ナビウォーク”, http://www.au.kddi.com/ezweb/service/ez_naviwalk
- [9] 中村智和, “工程管理に用いる位置探索システムの研究”, 2001年度東京大学大学院新領域創成科学研究科修士論文
- [10] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, “The cricket location-support system” In Proceedings of MOBICOM 2000, pp. 32-43 (2000)
- [11] 安田明夫: GPSの測位原理, GPSシンポジウム’99, pp. 191-214 1999.11 社団法人 日本航海学会 GPS研究会

- [12] R. Want, et. al., : “ Active Badge Location System ” , ACM Transactions on Information Systems, Vol. 10, No. 1, pp. 91-102 (1992)
- [13] 野間大輔：産業環境用位置計測端末の開発，2002年度東京大学大学院新領域創成科学研究科修士論文
- [14] <http://www.mlit.go.jp/>
- [15] A. R. Beresford and F. Stajano, ”Location privacy in pervasive computing,” IEEE Pervasive Computing, vol. 2, pp. 46-55, 2003.
- [16] 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.
- [17] BluetoothSIG,<http://www.bluetooth.com/bluetooth/>
- [18] BluetoothSIG, “ Anonymity modes, ” in Bluetooth 1.2 Draft 4 Part C,Section 4.1 ,2003.
- [19] I.Guvenc,C.T.Abdallah,R.Jordan,and O.Dedeoglu, “ Enhancements to RSS based indoor tracking systems using kalman filter, ” in Proc.of Intl.Signal Processing Conf.(ISPC),Dallas,TX,U.S.,2003.
- [20] Marco Gruteser, Dirk Grunwald, “ Anonymous usage of location-based services through spatial and temporal cloaking,” in Proc. of ACM MobiSys 2003 .San Francisco,CA,USA:USENIX,2003,pp.31 ?42.
- [21] B.Hoh and M.Gruteser, “ Protecting location privacy through path confusion, ” in First International Conference on Security and Privacy for Emerging Areas in Communication Networks ,Athens,Greece, 2005.
- [22] 中西健一, 高汐一紀, 徳田英幸,”粒度の動的変更による位置匿名性についての考察”, 情報処理学会 マルチメディア、分散、協調とモバイルシンポジウム (DICOMO)
- [23] 3GPP2/TSG-C.R1002, “ 1xEV-DV Evaluation Methodology (V14) ” , June 2003.

- [24] ETSI TR 101 329-6 V2.1.1, “ Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; End-to- end Quality of Service in TIPHON systems; Part 1: General aspects of Quality of Service (QoS)
- [25] A. Pfitzmann, M. K, and hntopp, ”Anonymity, unobservability, and pseudonymity a proposal for terminology,” in International workshop on Designing privacy enhancing technologies: Springer-Verlag New York, Inc., 2001, pp. 1–9.
- [26] David Chaum, “ Untraceable electronic mail, return addresses, and digital pseudonyms ” In Communications of the ACM 4(2), February 1981.
- [27] A. Serjantov and G. Danezis, ”Towards an information theoretic metric for anonymity,” presented at Privacy Enhancing Technologies, 2002.
- [28] M. K. Reiter and A. D. Rubin, “ Crowds: Anonymity for Web Transactions ” , ACM Transactions on information and System Security, 1(1): pp66-92,Nov. 1998
- [29] Andrew, Serjantov “ On the anonymity of anonymity systems ” , Ph.D. Thesis
- [30] L. Sweeney. :k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 2002
- [31] EPCglobal, <http://www.epcglobalinc.org/>
- [32] 鈴木雅貴, 山根弘, 黄樂平, 今井秀樹, 古原和邦, 松浦幹太, “プライバシ保護技術の評価フレームワークに関する検討,” The 28th Symposium on Information Theory and Its Applications (SITA2005)
- [33] A. Juels, “Minimalist Cryptography for RFID Tags,” 4th Conf. Security in Comm. Networks (SCN), C. Blundo and S. Cimato, eds., Springer-Verlag, 2004, pp.149-164
- [34] hingo Kinoshita, Fumitaka Hoshino, Tomoyuki Komuko, Akiko Fujimura and Miyako Ohkubo, “Nonidentifiable Anonymous-ID Scheme for RFID Privacy Protection,” Computer Security Symposium 2003 (CSS 2003)
- [35] S.Garfinkle and B.Rosenberg, RFID: Applications, Security, And Privacy .Addison-Wesley Pub-lisher, 2005.

- [36] S.L.Garfinkel,J.Ari,and R.Pappu, “ Rfid privacy:an overview of problems and proposed solutions,” Security and Privacy Magazine,IEEE ,vol.3,no.3,p.34,2005,1540-7993.
- [37] Stephen August Weis,”Security and Privacy in Radio-Frequency Identification Devices”,Master thesis,MASSACHUSETTS INSTITUTE OF TECHNOLOGY,2003
- [38] 個人情報保護に関する法律 (平成十五年法律第五十七号)
- [39] T.Camp,J.Boleng,and V.Davies, “ A survey of mobility models for ad hoc network research, ” Wireless Comm.and Mobile Computing (WCMC),vol.2,no.5,pp.483-502,2002.