現実世界の制約を考慮したRFIDシステムのリンク不能性に関する考察

野原, 康伸
九州大学大学院システム情報科学府

井上, 創造
九州大学大学院システム情報科学研究院

安浦, 寛人
九州大学大学院システム情報科学研究院

出版情報：コンピュータセキュリティシンポジウム CSS2006, pp.495-500, 2006-10
バージョン：
権利関係：

現実世界の制約を考慮したRFIDシステムのリンク不能性に関する考察

野原　康伸† 　　井上　創造‡ 　　安浦　寛人‡

†九州大学大学院 システム情報科学府
816-8580 福岡県春日市春日公園 6-1
nohara@c.csce.kyushu-u.ac.jp

‡九州大学大学院 システム情報科学研究院
816-8580 福岡県春日市春日公園 6-1
{sozo,yasuura}@c.csce.kyushu-u.ac.jp

あらまし RFIDシステムにおいて，ハッシュ関数等を用いてRFIDタグの出力を毎回変更し，タグ出力間のリンクを困難にすることにより，第三者によるユーザの位置追跡を防止する方式が提案されてきた．しかしながら，タグ出力と同時に観測される位置情報には，現実世界の制約のため強い相関が存在する．このため，第三者による位置追跡の危険性が依然としてあるといえる．本発表では，現実世界の制約を考慮したRFIDシステムのリンク不能性について議論し，第三者による位置追跡能力との関係について考察する．

A Study on Unlinkability of RFID System Considering Restrictions of Real World

Yasunobu NOHARA† 　　Sozo INOUE‡ 　　Hiroto YASUURA‡

†Graduate School of Information Science and Electrical Engineering, Kyushu University
6-1 Kasuga-koen, Kasuga-shi
Fukuoka, 816-8580 Japan
nohara@c.csce.kyushu-u.ac.jp

‡Faculty of Information Science and Electrical Engineering, Kyushu University
6-1 Kasuga-koen, Kasuga-shi
Fukuoka, 816-8580 Japan
{sozo,yasuura}@c.csce.kyushu-u.ac.jp

Abstract Unlinkability, the property that prevents an adversary recognizing whether outputs are from the same user, is an important concept in RFID. There are many proposed schemes that provide unlinkability, however most of the schemes don't consider restrictions of the real world. In this paper, we discuss the unlinkability of RFID systems considering restrictions of the real world.

1　はじめに

RFID(Radio Frequency IDentification) システムとは，無線通信が可能な小型IC(**RFIDタグ**) を用いて，人や物の識別をするシステムのことである．RFIDタグを用いることにより現実世界の人や物に電子的な識別子をつけ，現実世界の情報とデータベース上の仮想世界とを対応づけることが可能となる．RFIDシステムは，どこにでも計算機が存在する環境を意味するユビキタスコンピューティングの根幹をなす基盤システムとして期待が大きい．

RFIDシステムでは無線により通信が行われるため，第三者がユーザに気づかれることなく無断でRFIDタグ上のIDを収集することができる．このため，第三者が様々な場所にリーダを設置し，ID等を紐付けすることにより第三者がユーザの行動を追跡できてしまうという問題がある．この問題の解決方法として，情報の送信元が同一の人物によるものであるかを判定で

きないという**リンク不能性**(Unlinkability) を実現する方法があり，筆者らの方式を含め [1, 2]，様々な方式が提案されてきた [3, 4]．これらの方式におけるリンク不能性とは，正確に言えば「ID から同一人物であるか判断することが困難」であるということであった．

一般に，RFID タグの出力を観測する際，ID の情報と共に，観測時刻と観測場所を取得することができる．ある RFID タグについての観測時刻と観測場所の複数ペア同士には，現実世界の制約のため，強い相関がある [5, 6, 7]．よって，第三者による ID のリンクを防止できるとしても，第三者によるユーザの位置追跡の危険性は残っているといえる [7]．

そこで本稿では，現実世界の制約を考慮することにより第三者による位置追跡の危険性がどのくらい高まるのかを議論する．まず，現実世界の制約を考慮した RFID システムのリンク不能性について考察する．そして，位置追跡モデルを提案し，位置追跡の一問題としてリンク問題を定義する．その後，リンク不能性と第三者による位置追跡能力との関係について考察する．

2 現実世界の制約を考慮したRFIDシステムのリンク

2.1 ロケーションプライバシー問題

RFID に関するプライバシー問題として，第三者がユーザの行動を追跡できてしまうロケーションプライバシー問題が知られている．第三者によるユーザの行動追跡方法は次の通りである．

Phase1: 第三者は各種場所にリーダを設置する．

Phase2: ユーザーが所有するタグがリーダの近くを通る度に，RFID タグの出力をリーダを用いて観測する．第三者は，観測されたタグ出力と同時に，タグ出力を観測した時間，および観測したリーダが設置された場所をデータベースに記録する．

Phase3: データベースからタグ出力等をキーとして，ある人物についての行動履歴である (観測時間，観測場所) の組を取り出す．

2.2 単純なリンク

RFID タグが毎回固定された ID を出力する場合，同一の ID を持つ (観測時間，観測場所) の組をデータベースから取得することにより，第三者は，Phase3 の作業 (以下，**リンク作業**) を行うことができる．すなわち，ある人物についての行動履歴を取得することができてしまう．

そこで，RFID タグの出力をハッシュ関数等を用いて毎回変化させることで，第三者には出力同士の関係が分からないようにする，つまり**リンク不能にする**手法が，筆者らの方式を含めて [1, 2]，提案されてきた [3, 4]．これらの手法により，第三者がタグ出力を用いてリンク作業を行うことが事実上不可能となり，第三者による位置追跡は防止できるとされてきた．

2.3 現実世界の制約を考慮したリンク

前節でタグ出力を用いたリンク作業について述べたが，第三者がリンク作業に用いることができるのはタグ出力に限られない．一般に，ある RFID タグについての観測時刻と観測場所のペアには，

- ある地点にある物は，時間がそれほど経過していなければその近傍に留まり，遠方には存在しない
- ある地点にある物は，別のある地点を必ず通らなければならない，又は通ってはいけないというルール

といった現実世界の制約により強い相関が存在する [5, 6, 7]．よって，この相関を利用することにより，次の例のように第三者によるユーザの位置追跡は起こり得ると考えられる [7]．

タグが 2 個しか存在しないようなシステムを考える．ある時刻 t において A 地点と B 地点に設置してあるリーダが，時刻 $t+k$ において C 地点と D 地点に設置してあるリーダが反応したとする．A 地点と C 地点は，距離が離れており時間 k で移動することは難しいとする．この場合，タグ出力が固定であっても可変であっても，ある人物が A 地点から D 地点へ移動し，もう一人が B 地点から C 地点へ移動したことが分かってしまう．

2.4 リンクの確率的表現

2.2 節におけるリンクでは，ある 2 組のタグ出力が同一のタグから出力されたものかどうか (リンクしているか) を，(1) 固定 ID の場合のように，100%の正解率で言い当てることができるか，(2) ハッシュ関数等により出力を変化させる場合のように，当てずっぽうと同じ正解率しかだせないか，の 2 つに 1 つであった．

しかしながら，現実世界の制約を利用したリンクの場合には，そのリンクの度合いには不確実性が存在し，確率的に表現することになる．例えば，時刻 t に地点 A で観測された人物と RFID タグが，時刻 $t+k$ に地点 B に移動する確率は 0.3，地点 C に移動する確率は 0.1 といった具合である．

リンクの確率的表現を用いることにより，現実世界の様々な制約を取り込むことができる．例えば，A 地点から B 地点に時間 k で移動することが難しいという制約は，(時刻 t, 地点 A) という組と (時刻 $t+k$, 地点 B) という組のリンクの度合いとして 0 に近い値を設定すればよい．

2.5 比較

既存のリンクと本論文で扱うリンクの相違点をまとめると表 1 のようになる．

表 1: 既存のリンクと本論文のリンクの比較

	既存	本論文
リンクの対象	ID のみ	ID, 位置情報, 時間情報
リンクの表現	あるかないか (0 or 1)	確率 (0 以上 1 以下)

3 現実世界の制約を考慮した位置追跡モデル

本章では，攻撃者の RFID を用いた人や物の位置追跡能力を評価するため，現実世界の制約を取り込んだ位置追跡モデルについて説明する．

3.1 モデル化の対象となるシステム

N 個の RFID タグが人や物に取り付けられ，r 個のリーダが存在し，RFID タグが m 箇所の場所を動いている場合を想定する．

RFID タグが移動できる場所 l_i の集合を L とする．また，リーダが設置している場所の集合を $L_R \subseteq L$ とする．

リーダは，RFID タグが通信可能範囲に入った場合において，

1. リーダが RFID タグの出力を正しく読み取る
2. リーダと RFID タグの間に遮蔽物がある等の理由で，リーダは RFID タグの存在をまったく検知できない (False negative)

のいずれかの動作をするものとする．それぞれが起こる確率を，$1-P_{err}$, P_{err} とする．

なお，RFID タグが存在しないのにリーダが RFID タグの存在を誤検知してしまう False positive の発生は考えないものとする．

3.2 現実世界の制約を考慮した位置追跡モデル

図 1 に現実世界の制約を考慮した RFID による位置追跡モデルを示す．

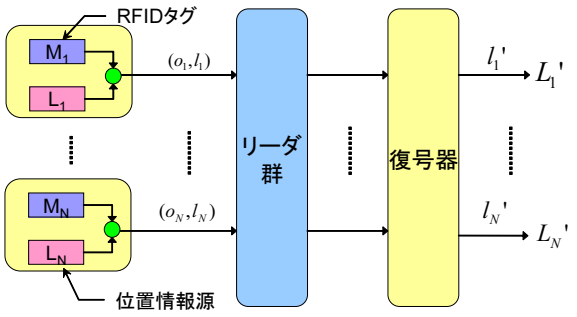

図 1: 現実世界の制約を考慮した位置追跡モデル

追跡モデルにおいては，RFID タグ M_i と位置情報源 L_i の N 個の組，r 個のリーダからなるリーダ群，復号器という要素が登場する．

以下では，各要素について説明する．

3.2.1 RFID タグと位置情報源

人や物に取り付けられた RFID タグ M_i が，様々な地点 $l_i \in L$ を移動することを RFID タグ M_i と位置情報源 L_i のペアによって表現する．ここで，位置情報源 L_i は，RFID タグ M_i が存在する場所を表す情報源であり，情報源アルファベットとして L を取る．

位置情報源としてマルコフ情報源を用いれば，状態遷移確率の設定により，先に示した現実世界の制約をモデル中に取り込むことができる．

本稿では，取り扱いの容易性を考え，位置情報源として単純マルコフ情報源を採用するものとし，時間 k の間に人が位置 i から位置 j へ移動する確率を $q^k(i,j)$ と表現する．

3.2.2 リーダ群

図 1 の追跡モデルにおけるリーダ群は，N 組の (O_i, L_i) を入力とし，N 組の $(O_i \cup \{*\}, L_i \cup \{*\})$ の出力を行うアルゴリズムとして表現される．ここで $*$ は，O_i または L_i のどの要素であるか不明であることを表す．本アルゴリズムで出力されるものが，Phase2 でデータベースに格納される (出力，場所，時間) の組に対応している．リーダ群の動作は以下のように記述される．

Step1: $i = 1$ とする

Step2: M_i からの入力を o，L_i からの入力を l とする．

Step3: $l \notin L_R$ ならば，$Z_i = (*, *)$ として Step6 へ

Step4: $x = GenRandReal(0, 1)$ とする

Step5: $0 \leq x < P_{err}$ ならば $Z_i = (*, *)$，さもなければ $Z_i = (o, l)$ とする

Step6: $i \neq N$ ならば $i = i + 1$ として，Step2 へ

Step7: $i = 1$ とする

Step8: $j = GenRandInt(i + 1, N)$ とする

Step9: Z_i と Z_j のデータを交換する

Step10: $i = N - 1$ ならば，$Z_1, \cdots, Z_N$ を出力して終了する．さもなければ，$i = i + 1$ として Step8 へ

ここで，$GenRandReal(x, y)$ は x 以上 y 以下の実数の乱数を出力する関数，$GenRandInt(i, j)$ は i 以上 j 以下の整数の乱数を出力する関数を表す．

Step2,3 は，リーダの存在しない場所にある RFID タグの出力とその位置情報は取得できないことを表現している．Step4 から Step6 は，リーダが存在する場所にタグがいた場合に，タグの出力とその位置をリーダが読み取れる場合と，タグの RFID の出力が読み取れなかったりする場合を表している．

Step7 から Step10 は，データの並びのシャッフルを行い，Z_i からえられる位置情報 L_i に相関が生じないようにしている．

3.2.3 復号器

復号器とは，N 組の $(O_i \cup \{*\}, L_i \cup \{*\})$ を入力とし，N 個の位置情報 L_i を出力する有限状態機械である．攻撃者は，エラーで欠損したり，シャッフルされたデータ組を，データ間の相関を利用して補正したり，並び替えることによって，復号器の出力を位置情報源の出力にできるだけに近づけようとする．どれだけ近づけることができるかが，攻撃者の持つ位置追跡能力を現している．

3.3 位置追跡問題

位置追跡モデルにより，以下のように位置追跡に関する様々な問題が定義できる．

1. どのようにして，追跡能力が最大になるような復号器を作成するか
2. リーダの設置できる数が限られている場合に，いかにして追跡能力を高めるようにリーダを配置するか
3. リーダの読取エラー率により，追跡能力がどの程度変化するのか

次章では，$P_{err} = 0$ と条件を限定した 1 の問題 (リンク問題) について考察を行う．

4　リンク問題

4.1　定義

$P_{err} = 0$ とし，時刻 t と時刻 $t+k$ に得られた n 個の位置情報の集合をそれぞれ S, E とする．このとき，各人物の移動地点の正しい組み合わせを求める問題をリンク問題とする．

移動地点の組み合わせを全単写 $f : S \to E$ により表現する．時刻 t における位置 i と時刻 $t+k$ における位置 j のリンクの度合いは，$p^k(i,j)$ で与えられるものとする．このとき，ある適当な f を定めたときに，その組み合わせが正しい確率は，ベイズの定理より，

$$\frac{\prod_{s\in S} p^k(s, f(s))}{\sum_{g\in F}\{\prod_{s\in S} p^k(s, g(s))\}} \qquad (1)$$

となる．ただし，F は全単写関数の集合である．

攻撃者としては，(1) 式を最大とするような f を復号器とすると考えられる．(1) 式の分母は f によらず一定であるので，リンク問題は次のように言い換えることができる．

リンク問題

サイズが共に n であるような 2 つの集合 S, E と重み関数 $P : S \times E \to R^+$ が与えられたとき，コスト関数

$$C(f) = \prod_{s\in S} P(s, f(s)) \qquad (2)$$

を最大とする全単写 $f : S \to E$ を求めよ．

4.2　解法

リンク問題を総当り法により解こうとすれば，$O(n!)$ の計算時間を必要とする．

一方，(2) 式で表されるコスト関数において，直積が総和の形に変わっただけの割当問題は，ムンクルス・アルゴリズムにより $O(N^3)$ の計算時間で解くことができる [8].

(2) 式の対数を取ると，

$$\log(C(f)) = \sum_{s\in S} \log\{P(s, f(s))\} \qquad (3)$$

となる．$\log(W(i,j)) = W'(i,j)$ とおけば，割当問題と同じ形になる．

$\log(x)$ は単調増加関数であり，$x < y \iff \log(x) < \log(y)$ が成り立つので，(3) 式を最大とするような $\hat{f}$ は，(2) 式も最大とすることが保証される．

よって，リンク問題はムンクルス・アルゴリズムにより $O(n^3)$ の計算時間で解くことができる．

5　シミュレーション実験

筆者らの研究室をモデルとして，攻撃者が ID 情報なしで ($q^k(i,j) = p^k(i,j)$ とした場合)，どのくらいリンクを成功させることができるかのシミュレーション実験を行う．研究室の様子を図 2 にを示す．

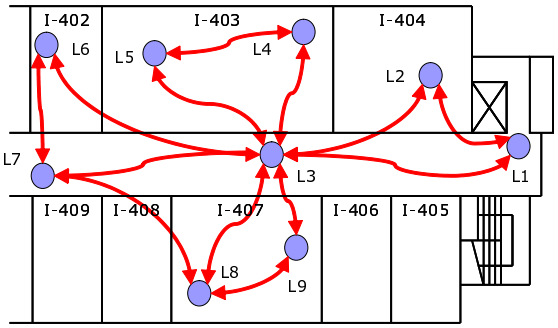

図 2: シミュレーション実験のモデルとなる筆者らの研究室

移動可能地点数 m，リーダ設置数 r を共に $m = r = 9$ とする．また，状態遷移行列 $\Pi = \{q_{i,j}\}$ を以下のように設定する．

$$\Pi = \begin{bmatrix}
0.1 & 0.2 & 0.7 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 \\
0.1 & 0.7 & 0.2 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 \\
0.2 & 0.1 & 0.1 & 0.1 & 0.1 & 0.1 & 0.1 & 0.1 & 0.1 \\
0.0 & 0.0 & 0.1 & 0.6 & 0.3 & 0.0 & 0.0 & 0.0 & 0.0 \\
0.0 & 0.0 & 0.1 & 0.3 & 0.6 & 0.0 & 0.0 & 0.0 & 0.0 \\
0.0 & 0.0 & 0.1 & 0.0 & 0.0 & 0.1 & 0.6 & 0.2 & 0.0 \\
0.0 & 0.0 & 0.1 & 0.0 & 0.0 & 0.2 & 0.7 & 0.0 & 0.0 \\
0.0 & 0.0 & 0.1 & 0.0 & 0.0 & 0.1 & 0.0 & 0.6 & 0.2 \\
0.0 & 0.0 & 0.1 & 0.0 & 0.0 & 0.0 & 0.0 & 0.3 & 0.6
\end{bmatrix}$$

ここで，状態遷移行列 Π は，部屋の中 (L2, L4, L5, L6, L8, L9) にいる場合，その場所に留まる可能性が高くし，廊下 (L1, L3, L7) にいる場合は，別の場所に移動する可能性を高くなる

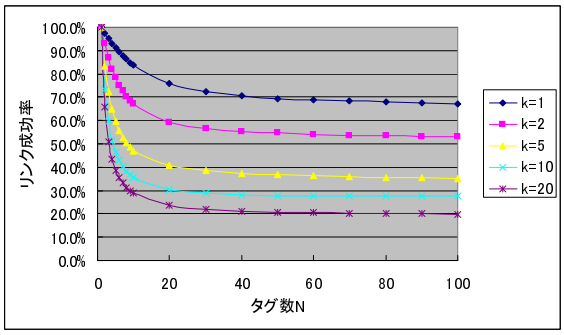

図 3: タグ数 N, 時間間隔 k とリンク成功率

ように設定している (例: $q_{4,4} = 0.6$, $q_{1,3} = 0.7$). また，部屋間の移動 (例えば，L5 から L6) を直接することはできず，一度廊下に出なければならないことから $q_{5,6} = 0$ のように設定している．

Java においてシミュレーションプログラムを作成し，各測定ごとに 10 万回の試行を行い，リンク成功率について調べた．

図 3 に，タグ数 N，観測時間間隔 k とシステム認識率の関係を示す．タグ数 N が増えるほど，またリンクを行う位置情報の観測時間間隔 k が増えるほど，システム認識率が低下することが読み取れる．$N = 20$，$k = 1$ の場合において，システム認識率は 75.8%という高さを示しており，現実世界の制約を用いた場合ロケーションプライバシー問題が深刻になる可能性が懸念される．

6 おわりに

本稿では，現実世界の制約を考慮した RFID システムのリンク不能性について議論し，第三者による位置追跡能力との関係を考察した．

今後の課題としては，他の位置追跡問題を解決することが考えられる．また，実際のシステムにおいてどの程度のリンクが可能なのか実験を行いたいと考えている．

謝辞

本研究は，科学研究費補助金 学術創成研究 (平成 14-18 年度, 課題番号 14GS0218) 及び，科学研究費補助金 若手研究 (A) (平成 18-20 年度, 課題番号 18680009) によるものである．

参考文献

[1] Nohara, Y., Inoue, S., Baba, K. and Yasuura, H.: Quantitative Evaluation of Unlinkable ID Matching Schemes, in *2005 ACM Workshop on Privacy in the Electronic Society – WPES2005*, pp. 55–60, ACM Press (2005).

[2] Nohara, Y., Nakamura, T., Baba, K., Inoue, S. and Yasuura, H.: Unlinkable Identification for Large-scale RFID Systems, *IPSJ Journal*, Vol. 47, No. 8, pp. 2362–2370 (2006).

[3] Weis, S. A., Sarma, S. E., Rivest, R. L. and Engels, D. W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, in *1st International Conference on Security in Pervasive Computing – SPC2003*, Vol. 2802 of *LNCS*, pp. 201–212, Springer (2004).

[4] Ohkubo, M., Suzuki, K. and Kinoshita, S.: Cryptographic Approach to a Privacy Friendly Tag, in *RFID Privacy Workshop@MIT* (2003).

[5] Beresford, A. R. and Stajano, F.: Location Privacy in Pervasive Computing, *IEEE Pervasive Computing*, Vol. 2, No. 1, pp. 46–55 (2003).

[6] 萩原大輔, 井上創造, 安浦寛人：RFID 情報システムにおけるシステムレベルでの信頼性向上, 情報処理学会論文誌：データベース, Vol. 46, No. SIG8, pp. 37–47 (2005).

[7] 山根弘, 黄楽平, 松浦幹太, 瀬崎薫：Silent period を用いた RFID ロケーションプライバシー保護手法の提案, 2006 年暗号と情報セキュリティシンポジウム – SCIS2006 (2006).

[8] Bourgeois, F. and Lassalle, J.-C.: An extension of the Munkres algorithm for the assignment problem to rectangular matrices, *Communications of the ACM*, Vol. 14, No. 12, pp. 802–806 (1971).