マルチメディア通信と分散処理 97－26
コンピュータセキュリティ 8－26
（2000．3．22）

匿名通信を記述するためのフレームワークについて

北澤 繁樹* 双紙 正和* 宮地 充子*

*北陸先端科学技術大学院大学 情報科学研究科,
〒 923-1292 石川県能美郡辰口町旭台 1-1

あらまし
電子投票や電子商取引において必要とされる匿名通信プロトコルについて，現在盛んに研究がなされている．それらの匿名通信プロトコルでは様々な手法を用いてメッセージの送信者や受信者の匿名性を実現している．しかしながら，匿名通信として各々プロトコルの細部については異なるが概念的なところでは共通する部分を多く含んでいる．
本研究では，既存の匿名通信プロトコルの共通部分に着目しフレームワークのモデル化を行う．この提案方式を用いて既存の匿名通信プロトコルを記述することでプロトコルの解析，分類することを容易にすることが可能となる．

Framework of Anonymous Communication Protocols

Shigeki KITAZAWA* Masakazu SOSHI* Atsuko MIYAJI*

*School of Information Science, Japan Advanced Institute of Science and Technology,
1-1 Asahidai, Tatsunokuchi, Nomi, Ishikawa 923-1292, JAPAN

Abstract
So far many researchers have vigorously proposed anonymous communication protocols for electronic vote and electronic commerce. They have devised various schemes to provide anonymity of a message sender and a receiver. However, although the proposed schemes are different in protocol details, we can observe that they share certain similarities essentially.
In this paper, we propose a framework of anonymous communication protocols paying attention to such similarities. The framework gives us criteria and means to evaluate and classify the protocols to achieve users' anonymity.

1 はじめに

ネットワーク通信上のユーザの匿名性や位置情報プライバシを保護するために，数々の研究が行われてきた [1, 2, 3, 5, 4, 6]．これらの方式は，それぞれ独立に提案されたプロトコルであるが，多くの共通点を持っている．我々はこのような共通点を持つ従来の匿名通信プロトコルの本質とは，(1)Proxy，(2) グループ通信 (同報通信) の 2 点であると考えている．ここでいうグループ通信とは，グループ内やグループ間でメッセージを共有することを目的とした通信を指す．

本研究では，このような観点から匿名通信プロトコルを記述するためのフレームワークにを提案する．このようなフレームワークを考えることによって今まで難しかった匿名通信プロトコルの評価，分類をすることが可能となる．このフレームワークの記述力を確かめるために従来の匿名通信方式をモデル化する．さらにこのフレームワークの様々な側面を議論する．

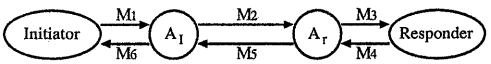

図 1: 一般的なメッセージ通信

2 匿名通信プロトコルのモデル化

2.1 実体

まず，以下のように定義する．

イニシエータ I: 送信内容 V を生成し送信を起動するユーザ

レスポンダ r: イニシエータが出す送信内容 V の最終的な宛先ユーザ

エージェント A: ユーザの代わりに実際の通信を行うプロセス．本研究では各ユーザにつきひとつのエージェントが存在するものとする

送信者 S; 受信者 R: ある通信リンク上において，直接通信を送信; 受信するユーザあるいはエージェントを表す．ただし，R がグループIDのときは，R はそのグループ全てのメンバを意味し，メッセージもそのグループメンバ全員にブロードキャストされるものとする

以上の定義をもとにすると，一般的な通信方式のメッセージ形式は (S, R, I, r, V) と定義することができる．メッセージ通信においては，I から r に到るまでの間に複数の中継ノードを介することがあるが，このとき，S，R は適宜変更されるものの，I，r，V は変更されない．以上をまとめて一般的な通信のモデルは，図 1で与えられる．ここで，A_I および A_r はそれぞれイニシエータ，レスポンダに対するエージェントである．また，ユーザとエージェントを合わせて実体とよぶ．

2.2 匿名通信プロトコルのモデル

本論文では，従来の匿名通信プロトコルの本質を (1)Proxy，(2) グループ通信 (図 2) の 2 点であると考える．すなわち，Proxy を利用した匿名通信プロトコルでは，イニシエータがメッセージを直接レスポンダに送るのではなく，通信路上に中継者 (Proxy) を設け間接的にレスポンダに送ることで，イニシエータを特定できないようにする．また，グループ通信による匿名プロトコルでは多

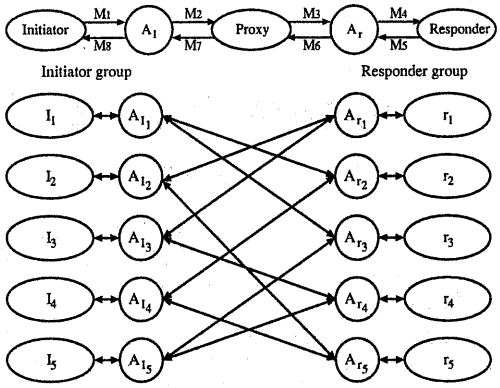

図 2: Proxy と多対多通信

対多通信の特性を利用することによって匿名性を実現している．これら 2 つの概念は独立しており，お互いを組み合わせることによって匿名性を向上させることが可能である．ネットワーク通信において考えられる匿名性は，(1) イニシエータのレスポンダに対する匿名性，(2) イニシエータの匿名メッセージ中継者に対する匿名性，(3) レスポンダのイニシエータに対する匿名性，(4) レスポンダの匿名メッセージ中継者に対する匿名性，があり，匿名通信はそのプロトコルによりこれらのうち 1 つ以上を必ず有する．

2.3 メッセージ形式

従来の匿名通信方式におけるメッセージ M は次の形式で表すことができる．

$$M = (S, R, PI, Pr, PV)$$

ここで，S, R はこのメッセージを直接送信，受信するユーザあるいはエージェントである．また，PI，Pr，PV は仮想的なパラメータを表している．これらは，それぞれ I，r，V における本来の情報を隠しつつ最終的なメッセージの到達可能性や返信可能性を確保するための要素である．

仮想的なパラメータは各匿名通信プロトコルによって様々な値をとる (表 1)．表 2の表記はそれぞれ，sid は通信セッションごとに割り振られるセッション ID，mid は個々のメッセージに対応するメッセージ ID，cid は環状経路において 1 つのメッセージに対して割り当てられる通信 ID，

匿名通信方式	PI	Pr	PV
Proxy	sid	r	V
MIX [1], Onion [6]	-	$E(mix_1, E(\cdots E(r, V)))$	
Crowds [5]	Path ID	r, mid	V
菊池方式 [3]	Group ID, mid	$E(k)\|E_k(V)$	
井上-松本方式 [2]	Group ID, mid	r	V
環状経路 [4]	Cyclic route, cid	E/C field	V

表 1: 仮想的なパラメータ

	通常通信方式	匿名通信方式
メッセージ形式	(S, R, I, r, V)	(S, R, PI, Pr, PV)
通信方式	A_I, A_r が中継	A_I, A_r などに加え, Proxy やグループ通信によって匿名性を実現 *

表 2: 通常通信方式と匿名通信方式の比較

V は V をいくつかに分解したセグメントの集合を表している.

一般的なメッセージ通信方式のメッセージ形式と比較すると表 2のようになる.

2.4 匿名通信関数

この節では, 既存の匿名通信方式を記述するために, 本研究で提案するフレームワークにおけるエージェントの挙動について議論する. このために, 受信したメッセージタイプにより次の送信先を決定し, 送信先へのメッセージを生成する匿名通信関数 F を導入する.

匿名通信プロトコル上のエージェントは受信したメッセージ M をどのように処理をするのかを, 各エージェントがメッセージを受信した時点で持っている状態によって判断しなければならない. 本研究では, エージェントが持つ状態を $\mathtt{DB}_r$: エージェントが受信したメッセージのデータベース $\mathtt{DB}_s$:エージェントが送信したメッセージのデータベースのようなデータベースに保存されている情報で表現する. これらのデータベースの要素はメッセージのタイプで分けられたデータベースである. 各実体が受信するメッセージのタイプは (Type1) イニシエータからエージェントへのメッセージ, (Type2) エージェントからエージェントへのメッセージ, (Type3) エージェントからレスポンダへのメッセージ, (Type4) レスポンダからエージェントへのメッセージ, (Type5) エージェントからイニシエータへのメッセージ, の 5 つである. 以上の議論に基づき, 関数 F は以下のように与えられる.

$DB_{s1}, DB_{s2}, DB_{s2}, DB_{s4}, DB_{s5} \in \mathtt{DB}_s$
$DB_{r1}, DB_{r2}, DB_{r3}, DB_{r4}, DB_{r5} \in \mathtt{DB}_r$
m: エージェントが受信したメッセージ
$type(m)$: 受信したメッセージのタイプを 1, 2, 3, 4, 5 で出力する関数
$\mathcal{M}$: エージェントが出力するメッセージの集合
Messages: $\mathcal{M}$ の集合

```
1   function F(m);
2    begin
3     Messages← ∅
4     x ← type(m)
5     DB_rx ← DB_rx + {m}
6     if (x = 1||x = 4) then /* line:12, 50 */
7      begin
8       M ← f_2(m, Key, DB_s, DB_r)
9       Messages←Messages+{M}
10      DB_s2 ← DB_s2 + {M}
11     end
12    else if (x = 2) then
13     begin
14      if g_2(m, Key, DB_s, DB_r) then
15       begin
16        if g_3(m, Key, DB_s, DB_r) then
17         begin
18          M ← f_{2,3}(m, Key, DB_s, DB_r)
19          Messages←Messages+{M}
20          DB_{s2,s3} ← DB_{s2,s3} + {M}
21         end
22        else if g_5(m, Key, DB_s, DB_r) then
23         begin
24          M ← f_{2,5}(m, Key, DB_s, DB_r)
25          Messages←Messages+{M}
26          DB_{s2,s5} ← DB_{s2,s5} + {M}
27         end
28        else
```

*(I, r, V) を変更しない中継エージェントが存在することもあるが, 匿名通信の議論とは無関係であるため省略した

```
29            begin
30              M ← f2(m, Key, DBs, DBr)
31              Messages←Messages+{M}
32              DBs2 ← DBs2 + {M}
33            end
34          endif /* line:16, 22, 28 */
35        end /* line:15 */
36      else if g3(m, Key, DBs, DBr) then
37        begin
38          M ← f3(m, Key, DBs, DBr)
39          Messages←Messages+{M}
40          DBs3 ← DBs3 + {M}
41        end
42      else if g5(m, Key, DBs, DBr) then
43        begin
44          M ← f5(m, Key, DBs, DBr)
45          Messages←Messages+{M}
46          DBs5 ← DBs5 + {M}
47        end
48      endif /* line:14, 36, 42 */
49    end /* line:13 */
50  endif /* line:12, 50 */
51  return(Messages)
52 end;
```

ここで，20行目の表記は，Type2の送信メッセージを DB_{s2} へ，Type3の送信メッセージを DB_{s3} へそれぞれ加える処理を表している．26行目も同様である．

$g_x(m, \mathrm{Key}, \mathrm{DB}_s, \mathrm{DB}_r)$ $(x = 2, 3, 5)$ は受信メッセージ m に対する出力を次にどの実体に対して送信するのかを，受信エージェントの持っている状態によって判断する関数であり，戻り値はtrueまたはfalseである．関数の添字 x はエージェントが受信するメッセージのタイプを表している．

$f_x(m, \mathrm{Key}, \mathrm{DB}_s, \mathrm{DB}_r)$ $(x = 2, 3, 5)$ は m のタイプと受信したときのエージェントの状態から次の実体に送信するためのメッセージを生成する関数である．メッセージの生成法は個々のプロトコルの仕様により決定される．

関数 g_x および関数 f_x の引数であるKeyはそのエージェントが管理する暗号化鍵と復号鍵の集合を表している．これらの鍵はメッセージ自体の暗号化や復号にも用いられるが，I や r を匿名にした場合の匿名通信方式においてデータを復号できるか否かで自分宛であるかを確かめるときにも用いられる．なお，本研究ではこれらの鍵の配送方式などについては言及しない．

また，関数 g_x および関数 f_x はエージェントの状態 $(\mathrm{DB}_s, \mathrm{DB}_r)$ に対する副作用をおよぼさないとする．すなわち，メッセージの生成順序による出力結果の差異は生じない．

7行目から11行目の処理は，エージェントが r または I からメッセージを受信したときの処理である．ただし，提案方式ではType1，Type4のメッセージを受信した場合，エージェント以外の実体へ次のメッセージ送信することは想定していないので，必ずType2の送信メッセージを出力する．

13行目から49行目の処理は，メッセージの送信元がエージェントであるメッセージを受信したときの処理である．このとき，エージェントが生成し得るメッセージタイプはType2，Type3，Type5の3タイプである．

17行目から21行目Type2とType3のメッセージタイプを同時に生成するような場合を考えている．同様に23行目から27行目では，Type2とType5のメッセージタイプに関する処理である．

51行目では，1回の処理で $F(m)$ が出力する全てメッセージを関数の戻り値として返す．ただし，Messages$=\emptyset$であった場合には，エージェントの状態は遷移するが，どの実体にもメッセージを送信しない．

3 既存方式の記述

この章では，既存の匿名通信方式のうち，多くのプロトコル要素を含む井上-松本方式 [2] について，提案フレームワークによるモデル化とプロトコルの記述を行う．その他の匿名通信プロトコルに関しては，井上-松本方式を応用することで記述が容易である．井上-松本方式に関する詳細は文献 [2] を参照されたい．

3.1 井上-松本方式モデル

井上-松本方式は以下のようにモデル化することができる．PI としては，グループID(G_A)とメッセージID(mid)を用いる．また，井上-松本方式ではレスポンダが個人である場合の匿名性はないので，Pr は常に r である．PV としては，イニシエータ，レスポンダが生成する通信内容 V，V と，V をいくつかに分解したのセグメントの集

合 V を用いる.

3.2 井上-松本方式モデルの記述

g_2, g_3, g_5 は以下のように定義できる.

g_2: 受信した m の PV が要素数 2 以上であるセグメントの集合であるときに真になる

g_3: 受信した m の PV が要素数 1 であるセグメントの集合でありかつ DB_{r2} に保存してあるメッセージの内, PI のメッセージ ID が等しいメッセージのセグメントが全てそろったときに真になる.

g_5: 受信した m の PI に, DB_{s2} に保存してあるメッセージ ID が含まれ, かつ PV にセグメントが含まれていないときに真になる

また, f_2, f_3, f_5 は以下のように定義できる.

f_2 : f_2 の出力は, 入力されたメッセージのタイプにより異なる.

Type1 のメッセージを受信した場合

$$f_2((I, A_I, I, r, V), \mathtt{Key}, \mathtt{DB}_s, \mathtt{DB}_r) = \begin{cases} (A_I, A_j, (G_A, mid), r, \mathtt{V}_1) \\ (A_I, A_k, (G_A, mid), r, \mathtt{V}_2) \end{cases}$$

ただし, j, k はグループ ID が G_A であるユーザの中から無作為に選ばれる. また $\mathtt{V}_1$ および $\mathtt{V}_2$ は, V を n 分割して順番をシャッフルした後, 無作為に 2 分割されたセグメントの集合を表している.

Type4 のメッセージを受信した場合

$$f_2((r, A_r, (G_A, mid), r, V'), \mathtt{Key}, \mathtt{DB}_s, \mathtt{DB}_r) = (A_r, G_A, (G_A, mid), r, V')$$

Type2 のメッセージを受信した場合

$$f_2((A_\alpha, A_\beta, (G_A, mid), r, \mathtt{V}_i), \mathtt{Key}, \mathtt{DB}_s, \mathtt{DB}_r)$$

$\mathtt{V}_i$の要素数が 1 のとき

$$= (A_\beta, A_r, (G_A, mid), r, \mathtt{V}_i))$$

$\mathtt{V}_i$の要素数が 2 のとき

$$= \begin{cases} (A_\beta, A_r, (G_A, mid), r, V_h) \\ (A_\beta, A_l, (G_A, mid), r, \mathtt{V}_i - \{V_h\}) \end{cases}$$

$\mathtt{V}_i$の要素数が 3 以上のとき

$$= \begin{cases} (A_\beta, A_r, (G_A, mid), r, V_h) \\ (A_\beta, A_l, (G_A, mid), r, \mathtt{V}_3) \\ (A_\beta, A_m, (G_A, mid), r, \mathtt{V}_4) \end{cases}$$

ここで, A_α, A_β をそれぞれあるエージェント間通信の送信側と受信側という意味で用いている. l, m はグループ ID が G_A であるユーザの中から無作為に選ばれる. $\mathtt{V}_3$ および $\mathtt{V}_4$ は, 受信したセグメントの集合 $\mathtt{V}_i$ から, A_r に送るセグメント V_h を引いた残りを無作為に 2 分割したセグメントの集合を表す.

f_3 : グループ G_A に所属する複数のエージェントから送られて来た n 分割されたメッセージ $V \leftarrow V_j$ $(j = 1 \sim n)$ から元のメッセージ V を復元し, レスポンダ宛のメッセージを生成

$f_3((A_\alpha, A_r, (G_A, mid), r, V_j), \mathtt{Key}, \mathtt{DB}_s, \mathtt{DB}_r) = (A_r, r, (G_A, mid), r, V)$

f_5 : レスポンダからグループ宛にブロードキャストされたメッセージを受信し, イニシエータ宛のメッセージを生成

$f_5((r, A_I, (G_A, mid), r, V'), \mathtt{Key}, \mathtt{DB}_s, \mathtt{DB}_r) = (A_I, I, (G_A, mid), r, V')$

4 考察

ここでは, 提案した匿名通信方式に関するフレームワークと, その妥当性についての議論を行う.

4.1 匿名通信関数 $F(m)$

匿名通信関数 $F(m)$ は, 通信路アーキテクチャを決定する関数 g_x と受信メッセージを元に送信メッセージを出力する関数 f_x で構成される. 本章では, これら 2 つの内部関数の型について考察する.

4.1.1 関数 g_x

関数 g_x $(x = 2, 3, 5)$ は, 受信したメッセージとエージェントの持つ状態から, 次のメッセージ送信先の実体を判定する. よって, メッセージの往信時に g_3(次の送信先がレスポンダであると判断する関数) が真になるステップが少なくとも

1回成立することは，その匿名通信方式におけるメッセージ到達可能性を意味する．同様に，返信時に g_5(次の宛先がイニシエータであると判断する関数) が少なくとも1回成立するか否かで，ある実体に対してイニシエータの匿名性を持たせた場合のメッセージ返信可能性を評価することができる．

4.1.2 関数 f_x

関数 f_x $(x = 2, 3, 5)$ は，受信したメッセージとエージェントの持つ状態から，次のメッセージ送信先へのメッセージを生成する関数である．よって，仮想的なパラメータを制御するのもこの関数の機能であるので，4.1.1節で述べたメッセージ到達可能性や返信可能性および4.2節で述べる匿名性にも深く関与する．

f_3 はメッセージの仮想的なパラメータとエージェントの持つ状態を用いて実際のレスポンダを特定する機能を持っている．同様に，f_5 にはイニシエータを特定する機能がある．

4.2 匿名性

関数 F の定義から分かるように，ある通信において $g_3(m, \mathtt{Key}, \mathtt{DB}_s, \mathtt{DB}_r)$ が真になったときその通信におけるレスポンダに対してメッセージを送ることができる．このメッセージは関数 f_x によって生成される．これを言い替えると $(\mathtt{DB}_s, \mathtt{DB}_r)$ の状態にあるエージェントはメッセージを得るとレスポンダに送るべきメッセージを構成できると言うことに他ならない．これはレスポンダの匿名性が失われる条件 (十分条件) を表している．イニシエータの匿名性についても同様である．

4.3 既存プロトコルの分類

本提案方式を用いて表1で挙げた既存の匿名通信プロトコルを分類したのが図3である．図3において，multicast，broadcast はそれぞれ井上-松本方式，菊池方式を表している．

5 むすび

本研究では，既存の匿名通信プロトコルの2つの独立した本質，Proxy とグループ通信に着目し，匿名通信プロトコルを記述するためのフレームワークを提案した．また，提案方式を用いて既存の匿名通信プロトコルを記述することにより匿名性が失われる場合の条件について考察した．本研究のモデル化を用いて既存の匿名通信プロトコルを記述することによりプロトコル匿名性を評価，分類することが可能となった．将来的には，匿名通信プロトコルをより詳細に記述できるようにすることで，既存のプロトコルの改良や新しいプロトコルの発見に利用することが期待できる．

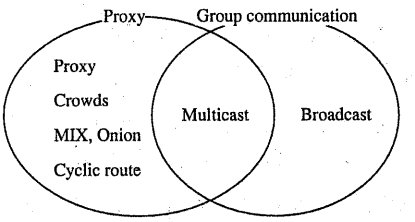

図 3: 既存匿名通信の分類

参考文献

[1] Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, *Communications of the ACM*, Vol. 24, No. 2, pp. 84–88 (1981).

[2] Inoue, D. and Matsumoto, T.: Anonymity Achieved by Group Communication, *Proc. IEICE JW-ISC2000* (ISEC-99-100).

[3] Kikuchi, H.: Sender and Recipient Anonymous Communication without Public Key Cryptography, 情報処理学会研究報告 (98-CSEC-1-8) (1998).

[4] 長野悟, 北澤繁樹, 双紙正和, 宮地充子: 環状経路を用いた匿名性と位置情報プライバシの保護, コンピュータセキュリティシンポジウム (CSS99), pp. 37–42 (1999).

[5] Reiter, M. K. and Rubin, A. D.: Crowds: Anonymity for Web Transactions, *ACM Trans. Info. Syst. Security*, Vol. 1, No. 1, pp. 66–92 (1998).

[6] Syberson, P. F., Coldschlag, D. M. and Reed, M. G.: Anonymous Connections and Onion Routing, *IEEE Symposium on Security and Privacy*, pp. 44–54 (1997).