

論文

無線端末向けデータ複製技術の開発

大原 衛*¹⁾ 岡野 宏*¹⁾ 河村 洋*¹⁾

A Data Replication Technique for Portable Wireless Terminals

Mamoru OHARA, Hiroshi OKANO and Hiroshi KAWAMURA

Abstract Providing information services via wireless networks is a promising way for helping outdoor activities for elderly and physically challenged persons. However, wireless network infrastructures, such as mobile cellular phone networks are still not as dependable as they could be. As an example of this, Internet access services on a mobile cellular phone network often suffer from service suspension due to failures on central server machines and network equipments. In this paper, we replicate important information into user terminals and network equipments near the users and use the replicas to continue services even in the event of such failures. We introduce a coding scheme using Redundant Residue Number System (RRNS) to replicate information. We implemented a prototype system with a Hypertext Transfer Protocol (HTTP) proxy using the RRNS coding scheme and confirmed that the replica could provide information instead of the servers that have failed.

Keywords dependable system, data replication, personal digital assistance (PDA), redundant residue number system, HTTP proxy

1. はじめに

携帯電話や個人情報端末（以下、PDA）を用いた無線通信による情報サービスは非常に広く普及しており、今後、高齢者・障害者支援用途への応用が期待されている。しかし、携帯電話を用いたインターネット接続サービスに代表される従来システムでは、サーバ、ネットワーク機器等の障害などによるサービス停止が、年数回程度の頻度で発生している。高齢者・障害者支援システムには通常の情報システム以上の信頼性が要求されるため、従来システムでは可用性が十分でない。本研究では、高齢者・障害者が安全に安心して利用できる情報サービスの構築のための、情報複製によるシステム高信頼化技術を開発した。

本研究の提案手法では、図1のように情報の複製をPDA自体やネットワーク上で利用者に近い無線中継機器等に保存する。サーバやネットワークに障害が発生した場合も、これらの複製を利用してサービスを継続できるようにする。通常、無線中継機器やPDAは、サーバやPCなどに比べて、計算性能や記憶容量の面で劣る。提案手法では、冗長剰余系を用いた情報符号化手法によって情報を符号化し、これらの機器に適した形態で情報の複製を保存する。

本手法の試験実装として、中継する情報を自動的に符号化し、複製として保存するHTTP（Hyper Text Transfer Protocol）プロキシを作成した。プロキシはサーバとサー

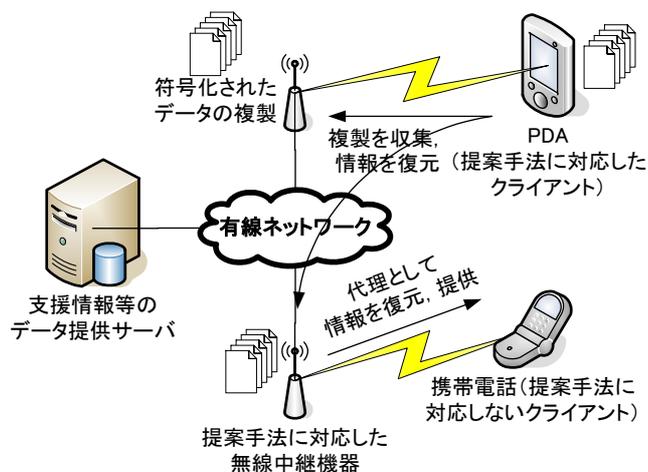


図1 提案手法の概念図

ビス利用者間の通信を仲介する。これによって通信手順の異なるホスト間の通信を実現できる。携帯電話のような新規機能の追加が比較的難しい機器に対しても、プロキシを利用することで、提案手法が適用可能となる。開発したプロキシは、既存のサーバおよびクライアントで構成されたシステムに複製による冗長性を導入する。これによって、障害発生時もサービスの継続が可能になることが示される。

2. 冗長剰余系

本研究では、計算性能、記憶容量の両面で制約の強い

*¹⁾ エレクトロニクスグループ

PDA 等での利用に適した情報符号化方式として、冗長剰余系を利用した符号化手法¹⁾をとりあげ、これを用いた試験実装システムを構築した。本節では、冗長剰余系について概説する。

h 個の互いに素な正整数の組 (m_1, m_2, \dots, m_h) ($m_1 < m_2 < \dots < m_h$) を考える。これら h 個の整数の積を $M = \prod_{k=1}^h m_k$ とする。また、任意の非負整数 $X (X \in [0, M])$ に対して、 x_k を m_k による X の剰余とする。すなわち、 x_k は下式を満たす。

$$x_k = X \bmod m_k. \quad (1)$$

本稿では、整数の組 (x_1, x_2, \dots, x_h) を除数の組 (m_1, m_2, \dots, m_h) による X の剰余表現と呼ぶ。また、 (m_1, m_2, \dots, m_h) による $[0, M]$ の整数の剰余表現の集合からなる系を (m_1, m_2, \dots, m_h) の剰余系と呼ぶ。

任意の剰余表現 (x_1, x_2, \dots, x_h) から、下式で表される中国剰余定理によって、対応する数 X を復元することができる。

$$X = \left(\sum_{k=1}^h x_k \frac{M}{m_k} b_k \right) \bmod M. \quad (2)$$

ここで、 b_k は、下式を満たす正の整数である。

$$\left(\frac{M}{m_k} b_k \right) \bmod m_k = 1. \quad (3)$$

上述の h 個の除数からなる組にさらに r 個の除数を加えた組 $(m_1, m_2, \dots, m_h, m_{h+1}, \dots, m_{h+r})$ を考える。除数の組 $(m_1, m_2, \dots, m_{h+r})$ による $[0, M]$ の整数の剰余表現 $(x_1, x_2, \dots, x_{h+r})$ の集合からなる系を範囲 M 、冗長度 $M_R = \prod_{k=h+1}^{h+r} m_k$ の冗長剰余系と呼ぶ。また、冗長剰余系における剰余表現をとくに冗長剰余表現と呼ぶ。冗長剰余表現を構成する剰余 x_1, x_2, \dots, x_{h+r} は、通常の剰余系と同様に式(1)から求められる。

$h+r$ 個の除数を用いた通常の剰余系では、 $[0, M \cdot M_R]$ の整数を表現できる。一方、冗長剰余系では、 $h+r$ 個の除数を用いて $[0, M]$ の整数を表現する。 r 個の除数は冗長であり、最大 r 個の剰余が失われても X を復元できる。

ある冗長剰余表現の $d (\leq r)$ 個の剰余が失われ、残る $h+r-d$ 個の剰余 $\{x'_1, x'_2, \dots, x'_{h+r-d}\} \subseteq \{x_1, x_2, \dots, x_{h+r}\}$ が得られたとする。 $x'_1, x'_2, \dots, x'_{h+r-d}$ に対応する除数をそれぞれ、 $m'_1, m'_2, \dots, m'_{h+r-d}$ とすると、元の数 X は下式から求められる。

$$X = \left(\sum_{k=1}^{h+r-d} x'_k \frac{M'}{m'_k} b'_k \right) \bmod M'. \quad (4)$$

ただし、 $M' = m'_1 m'_2 \dots m'_{h+r-d}$ であり、 b'_k は式(3)と同様にして求められる。

3. 冗長剰余系を用いたデータ複製

本研究の提案手法では、前節で述べた冗長剰余系を用いて、情報を符号化し、複製として保存する。符号化では、文字、画像等の一般の情報のビットパターンを2進整数と見なし、この数の冗長剰余表現を構成する $h+r$ 個の剰余と除数をそれぞれ異なる機器に保存する。復号の際には、これらの異なる機器に保存された剰余と除数を、ネットワークを通じて h 個以上収集し、式(4)を用いて元の情報を復元する。すなわち、提案手法は情報の複製を複数の機器に分散して保存する手法といえる。このようなデータ複製手法は、Chessa らによって提案された¹⁾。

このような情報符号化手法は、以下のような点で無線情報サービスに適していると言える。

- ① 一部の剰余の損失に耐えられる。無線通信は、通常、有線通信に比べて通信品質が低く、誤りの混入や情報の損失が比較的起こりやすい。冗長剰余系では、 r 個以下の剰余の損失があっても元の数を復元できる。また、受信した剰余が誤っていた場合は、これを検出し、訂正できる場合がある¹⁾。
- ② 符号化・復号化処理が単純であり、計算性能に劣る PDA 等での利用に適する。符号化は整数剰余演算で、復号化は整数積和演算と剰余演算によって実現できる。
- ③ 剰余は除数未満の非負整数となる。元の数よりも小さな除数を選択すれば、個々の剰余は元の情報よりも小さなデータサイズで表現可能である。PDA 等の記憶容量に制限のある機器への保存に適する。
- ④ 一部の剰余や除数を得ただけでは元の数を復元できない。たとえば除数を、情報を閲覧する権限を有するユーザだけが知りうる秘密とすれば、セキュリティの向上に寄与できる。

情報の複製をそのユーザの近辺に保存する手法は、静的な手法と動的な手法が考えられる。静的な手法は、主に環境に設置されたネットワーク機器等を対象として、各機器の障害発生頻度等を考慮し、あらかじめ計画的に複製を配置する。これに対して、動的な手法では、たとえばユーザが用いる PDA が過去に参照した情報の複製を保存しておくことが考えられる。この場合、頻繁に参照される情報(たとえば周辺地図など)については、その複製を保持した PDA が周辺に存在する可能性が高い。一方、あまり頻繁に参照されないが重要な情報の複製には、静的な手法を併用する必要がある。

PDA やその通信を中継する機器は、それぞれ異なる除

数に対する剰余を保持することが望ましい。冗長剰余系では、元の数 X を復元するために、 h 個以上の互いに素な除数と対応する剰余が必要である。同じ除数による剰余が複数あっても、高信頼化に直接寄与しない。通常、不特定多数のユーザの PDA を含む多くの機器が、すべて異なる除数を用いることを保証するのは難しい。機器固有の物理ネットワークアドレス等の情報を基にした乱数を発生させ、十分に大きな素数表から除数を選択するなどの手法によって、確率的に異なる除数を与えることができる。

4. 試験実装

4.1 試験実装の仕様

高齢者・障害者支援を目的とした情報サービスでは、文字情報に加えて音声や映像情報が多用されると思われる。HTTP²⁾は、このようなマルチメディアデータの伝送にもっとも広く用いられている。また、携帯型情報端末への HTTP の普及も著しく、ほぼすべての携帯電話や PDA に、これに対応したブラウザが搭載されている。今後、高齢者・障害者支援情報システムが展開される際には、HTTP は情報伝送プロトコルとしてもっとも有力な候補であると言える。このため、本研究では、HTTP を情報伝送プロトコルとして試験実装を行った。

このような広く普及した手法に新規に機能を追加する際には、この機能を扱えない従来機器との互換性に留意する必要がある。本研究では、従来の機器を直接修正して機能を追加するのではなく、図 2 に示したように、プロキシと呼ばれる情報中継を担うモジュールをシステムに追加し、これに冗長剰余系による情報符号化機能を実装した。プロキシは、提案手法に対応したホストと対応しない従来のホストの通信を仲介し、相互に互換性を持たせる。

図 2 でサーバおよびクライアントは、提案手法に対応している必要はない。HTTP には、プロキシを介してサーバと通信する手順が規定されている。図のクライアントは、提案手法を適用したプロキシを利用するように設定される。このように設定されたクライアントは、HTTP 要求をサーバに直接送らずに、プロキシに送信する。

提案手法では、通常運用時において、図 2 の 1→2a→3~6 の順に情報が伝送される。プロキシは、サーバと通信が可能であれば、クライアントの要求を単にサーバに転送する。サーバはこの要求に応え、指定された情報をプロキシへ応答として返送する。プロキシは、この情報を前節で述べた手法によって符号化し、複製として保存した後に、応答をそのままクライアントへ転送する。すなわち、試験実装は、動的に複製を生成し、配置する。

サーバやネットワークの障害によって、サーバとの通信が断絶された状態で要求を受信した場合、プロキシはブロードキャスト型通信を用いて付近の機器に複製の有無

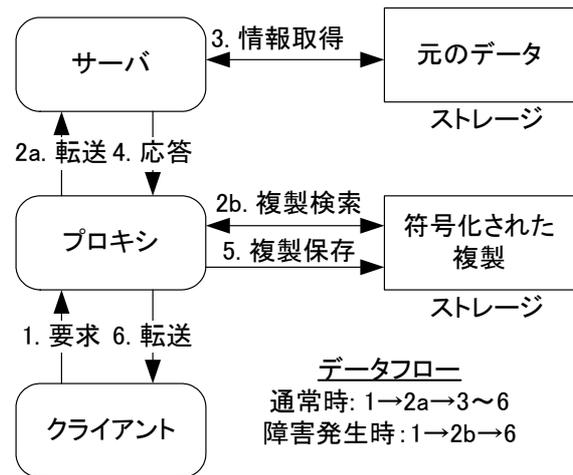


図 2 試験実装システムのデータフロー図

を問い合わせる。プロキシを動作させる機器自身を含めた複製を保有している機器は、これをプロキシに送信する。十分な数の複製が収集できた場合は、プロキシは元の情報を復元し、これをクライアントに送信する（図 2 の手順 1→2b→6）。複製の数が不十分であったときは、クライアントにエラーを通知する。

プロキシは、無線中継機器やユーザの利用する PDA 上に実装される。提案手法は、PDA と無線中継機器の両方でプロキシが動作するシステムで効果的に機能する。このようなシステムでは、PDA 自体が複製を保持できるため、システムのユーザが増えるほど冗長性が増し、システム可用性が向上する。しかしながら、携帯電話などを含めた、より広範な機器をユーザが利用できることが望ましい応用では、これらの機器に新規にプロキシを導入するのが難しい場合がある。このような場合は、無線中継機器にプロキシを導入し、これが携帯電話等の非対応機器との通信を仲介することで、本手法を適用できる。この場合、サーバやネットワークの障害に対しては、無線中継機器上のプロキシが複製を利用してサービスを提供することが可能であるが、無線中継機器が故障すると非対応機器に対するサービスは停止する。

4.2 HTTP への適用

HTTP のメッセージは図 3 に示したような形式をとる。すなわち、HTTP メッセージは、先頭行 (start-line)、ヘッダ (message-header)、内容 (message-body) から構成される。先頭行は要求及び応答コード等を含み、詳細は内容として与えられる。ヘッダは、後述する TE ヘッダフィールド等のオプションを含む。試験実装では、肯定応答メッセージの内容のみを符号化し、保存した。

メッセージの内容が、冗長剰余系を用いて符号化されていることを示すために、TE (Transfer Encoding) ヘッダフィールドを用いた。TE ヘッダフィールドは、HTTP で通信を行うホスト同士が、メッセージ内容の通信路符号化方式

```
generic-message
= start-line
*(message-header CRLF)
CRLF
[ message-body]
TE = "TE" ":" #( t-codings)
t-codings = "trailers" | (transfer-extension)
```

図3 HTTPメッセージの形式(抜粋)²⁾

を指定するために用いられる。TEヘッダフィールドの使用例を図4に示す。たとえば、TEヘッダフィールドに“deflate”が指定されていた場合、通信路符号化にgzipが用いられることを示す³⁾。試験実装では、TEヘッダフィールドに非標準の拡張“RRNS”を指定して、冗長剰余系による符号化を示すこととした。HTTPには、非標準拡張に対応しないホストが、これを無視し、代替として対応可能な方式を指示する手順が規定されている。このため、提案手法を適用したホストは、従来のホストと互換性を持つ。

図4の例に示したように、試験実装では、TEヘッダフィールドの引数として、符号化に用いた除数を与える。試験実装は、提案手法による信頼性の向上を確認することを主眼としたため、セキュリティに関する配慮はとくに行わなかった。

| | |
|--------------------|--------|
| TE: deflate | (gzip) |
| TE: RRNS, moduli=3 | (提案手法) |

図4 TEヘッダフィールドの使用例

4.3 試験実装機と通信実験

図5のような組込み機器とPDAを試験実装機として、これらに提案手法を適用したプロキシを導入し、通信実験をおこなった。これらの機器は、LinuxをOSとする。通信実験では、PDAに標準で導入されているWWWブラウザを、HTTPクライアントとして利用した。また、HTTPサーバには、PC上で動作する既存のソフトウェアを利用した。クライアント、サーバともに、提案手法には対応していない。図の組込み機器やPDA上で動作するプロキシが、冗長剰余系による情報符号化機能を実現する。

まず、障害の存在しない状態で、開発したプロキシを介してクライアントとサーバが通信できることが確認された。また、この間にプロキシが符号化された情報の複製を保存することが確認された。

次いで、サーバを強制的に停止させた。この状態でクライアントが要求を送信すると、プロキシが保存された複製から情報を復元し、これを提供できることが確認された。この通信実験を、プロキシをPDA(図右)上または中継

機器(図左)上で動作させた場合についてそれぞれ行い、両方で同様の結果を得た。中継機器だけにプロキシを導入し、利用者端末であるPDAは本手法に対応しない場合でも、サービスの高信頼化が可能であることが示された。



図5 通信実験で用いた機器

5. まとめ

冗長剰余系による情報符号化手法を用いたシステム高信頼化技術を開発し、試験実装を行った。試験実装では、情報符号化・復号化機能をプロキシに実装し、サーバおよびクライアントは従来のものを利用できるようにすることで、本手法の従来機器との互換性を確保した。試験実装システムは、情報伝送プロトコルとしてHTTPを用い、文字、音声、画像等を含む情報を提供できる。これを用いて通信実験を行い、サーバとの通信が不可能な場合も、開発したプロキシが複製を収集して情報を復元し、サービスを継続できることを確認した。

本稿の通信実験では、サーバ、クライアントおよびプロキシが物理的にもネットワーク的にも近接していた。これらの機器を高年齢・障害者支援システムが実際に運用される屋外に設置し、提案手法の有効性を検討することは、今後の課題である。

参考文献

- 1) S. Chessa and P. Maestrini, “Dependable and Secure Data Storage and Retrieval in Mobile, Wireless Networks,” Proc. IEEE 2003 Int’l Conf. Dependable Systems and Networks (DSN2003), pp. 207–216 (2003).
- 2) R. Fielding, et al., Hypertext Transfer Protocol – HTTP/1.1, RFC2616, IETF (1999).
- 3) P. Deutsch, GZIP File Format Specification Version 4.3, RFC1952, IETF (1996).

(原稿受付 平成17年8月3日)