

## 論文

## 視覚障害者移動支援システムに向けた分散多数決冗長技術の開発

大原 衛\* 岡野 宏\*\* 河村 洋\*\*\*

## A Distributed Voting Technique for Walking Support Systems for Visually Impaired People

Mamoru Ohara\*, Hiroshi Okano\*\*, Hiroshi Kawamura\*\*\*

Development of information technologies and networks enables us to support independent outdoor walking of visually impaired people by voice navigation using personal digital assistances (PDA) and wireless high-speed networks connected to the Internet. Many researchers are studying technologies for introducing into the walking-support systems features, which protect blind people from traffic hazards using dynamic information read from sensors. However, few reports about the dependability and safety of such technologies have been presented. In this paper, we propose a distributed voting technique for walking-support systems for visually impaired people. The proposed technique uses three identical sensor nodes, which monitor the same area, and votes between the outputs of the sensors in order to mask errors of one of the sensors. Past voting systems were typically constructed with tightly-coupled special devices, and thus, are difficult to use outdoors. In contrast, we construct the proposed system with COTS embedded computers and network devices. We connect the embedded computers with a common wired LAN and present information to the user via wireless networks. We implemented an experimental system and measured overheads for distributed voting. We found that the experimental system had high dependability and sufficient responsiveness for supporting pedestrians.

キーワード: 視覚障害者移動支援システム, ディペンダブルシステム, 分散多数決冗長方式

Keywords: Walking-support system for visually impaired people, Dependable systems, Distributed voting redundancy

## 1. はじめに

視覚障害者移動支援システムは, 視覚障害者に目的地までの経路や周辺の施設情報を案内し, 屋外での安全な移動を支援する。このために必要となる GPS, RFID 等を用いた自位置検出技術やネットワーク基盤に関する研究が数多く報告されている。また, 環境に様々なセンサを設置し, 交通や道路工事に関する情報を適時に提供する技術の研究が進められている。しかしながら, これらの要素技術の安全性, 信頼性に関する研究は, ほとんど報告されていない。本稿では, 視覚障害者移動支援システムのための高信頼化技術について議論する。

視覚障害者の歩行を支援する情報は, 静的な情報と動的に生成される情報に分類される。静的な情報の例として, 地図や施設情報などが挙げられる。動的な情報としては, ユーザ周辺の温湿度に基づく気象予測や, 車両の通行の有無などが想定される。これらは, 環境に設置されたセンサから得られた信号を情報処理することによって生成される。本研究では, 特に重要性の高い情報として, 車両の通行のようなユーザの危険の有無に関する情報の高信頼化技

術を提案する。

情報システムの信頼性向上技術は, ディペンダビリティ技術と総称される<sup>(1)</sup>。ディペンダビリティは, 冗長と分散の2つのパラダイムによって実現される。冗長手法は, システムに必要な最低限の構成要素に加えて, これらの故障に備えた追加的な要素を組み込む手法である。また, システムの構成要素を地理的に分散して配置することで, 電源の故障などの共通モード故障の影響を低減できる。

本研究では, 冗長手法の1つである多数決冗長方式に分散手法を組み合わせ, 視覚障害者移動支援システムを高信頼化する技術を開発した。具体的には, 環境に同一の事象を監視する複数のセンサを設置し, これらのセンサの出力を多数決することで信頼性の向上を図る。屋外に複数のセンサを設置する場合, これらの間の距離が離れている場合が考えられる。このため, 各センサをネットワークに接続し, 情報の交換を行う。このためのネットワークには, 既に広く普及しているインターネット技術を用いた LAN を採用する。後述するように, ネットワークを介した多数決には, 故障や遅延に伴う問題が存在する<sup>(2)</sup>。本研究では, 通信遅延の上限が定められる有線 LAN を無線 LAN と組み合わせることでこれに対応した。

ディペンダブルシステムの実現は, 通常, 追加的なコストを必要とする。このため, ディペンダビリティ技術は,

\* IT グループ  
\*\* エレクトロニクスグループ  
\*\*\* 城南支所

コストと障害の重大性のトレードオフを考慮して選択される必要がある。視覚障害者移動支援システムでは、ユーザにリアルタイムに情報を提供することが求められる。また、ユーザの判断を誤らせないように正確な情報を提供することが重要である。このようなリアルタイム性、正確性は、視覚障害者移動支援システムに本質的に重要であり、通常の情報システムに比べて、より高度なディペンダビリティが求められると言える。このため、本研究では、高度なディペンダビリティを実現する多数決冗長手法を基本として採用し、既存のネットワーク技術を応用することでコストの低減を試みている。

本稿の構成は、以下の通りである。2節では、関連する研究について概略を述べる。3節は、本研究で提案する分散多数決冗長手法について説明する。提案手法の試験実装を行った。4節では、この試験実装について述べ、試験実装を用いた実験の結果を報告する。5節は本稿のまとめを与える。

## 2. 関連研究

### 2.1 分散システムと故障モデル

一般に分散システムは、複数のプロセスとこれらを結ぶネットワークによって構成される。プロセスは、アルゴリズムを実行する主体であり、システム内で一意に識別できる。ネットワークは、各プロセスをどのように結ぶかによって様々なトポロジをとりうる。本稿では、ネットワークは論理的にメッシュ構造をとり、各プロセスは任意の他プロセスと通信できるものとする。

本稿では、プロセスの故障モデルとしてビザンチン故障を仮定する。ビザンチン故障は、プロセスが故障の影響で任意の振る舞いをするような故障モデルである。プロセスは故障によって、一切の動作を停止する場合もあるが、誤った、または正しい出力を行う場合もある。また、ネットワークも任意の故障を生じる可能性があるものとする。ただし、ユーザはプロセスの故障とネットワークの故障を区別できない。

### 2.2 多数決冗長方式

多数決冗長方式は、複数のプロセスが同一のタスクを実行し、その結果を多数決することで誤りをマスクする手法である。 $N$ 個のプロセスから成る分散システムを $N$ プロセスシステムと呼ぶ。 $N$ プロセスシステムでは、多数決によって $(N/2-1)$ 個のプロセスの故障をマスクできる。冗長度が2、すなわち2個のプロセスで多数決を行う場合は、誤りを検出することはできるが、これをマスクすることはできない。2プロセスシステムで誤りが検出された場合、通常、両方のプロセスがタスクを再実行する。このため、リアルタイム性が要求される応用では、即時に誤りを訂正できる $N \geq 3$ の多数決冗長システムが用いられる。冗長度の増加は、コストの増加に直接影響するため、 $N=3$ としたシステムが多く用いられている。このようなシステムをTriple Modular Redundancy (TMR) システムと呼ぶ。TMRシステムは、主に航空機や宇宙機、列車などの制御に用いられてきた<sup>(3)(4)</sup>。

従来のTMRシステムは、通常、特別なハードウェアによって構成されたため、通常のシステムに比べて非常に高いコストを要する。Pradhanらは、マルチプロセッサシステム上で、通常時は2個のプロセスで動作し、故障発生時のみ3個のプロセスを使用するシステム構成手法を提案した<sup>(5)</sup>。このシステムでは、平均的なシステムの冗長度は3未満であり、期待コストを低減できる。また、多数決冗長システムに時間冗長の概念を導入することで、2プロセスシステムで誤りマスクを可能とする手法も提案されている<sup>(6)</sup>。これらの手法では、通常実行時はTMRシステムと同等の性能を示すが、誤りが発生すると再計算を行うため、性能が低下する。このため、システムの冗長度に制約があり、TMRシステムよりもリアルタイム性が要求されない応用に適している。

前述したように、視覚障害者の歩行支援にはリアルタイム性が要求されるため、提案手法では常に3個のプロセスを動作させ、多数決を行う。一方で、専用のハードウェアを用いず、広く普及している組込み機器とインターネット技術を応用することで、追加的なコストの発生を抑える。

### 2.3 分散多数決冗長方式

分散環境における多数決は、分散合意問題に帰着される。分散合意問題は、システム内の各プロセスがそれぞれ独自に0または1のいずれかの値を提案し、正常な全プロセスがどちらかの値に合意するような問題を言う。非同期分散システムにおいてプロセスまたはネットワークに故障が発生しうる場合、分散合意問題を解く決定性アルゴリズムは存在しないことが示されている<sup>(2)</sup>。このため、現実的なシステムでは、一定の制約を設けて分散合意問題を解くことが多い。多くの非同期分散システムで用いられている代表的な手法として、ハートビートがある。正常なプロセスは、定期的に他プロセスにメッセージを送信する。このメッセージが一定時間以上受信されない場合、プロセスが故障によって停止している確率が高いと考えられる。本研究でもセンサノードの故障停止の検出にハートビートを用いている。

誤りが検出されたプロセスは、回復処理を行う。固定故障に対しては、機器の交換などを必要とする場合がある。本研究では、一時故障が生じたプロセスは、一定時間後に正常状態に自動復帰すると仮定する。

## 3. 提案手法

本稿では、図1に示すような構成の視覚障害者移動支援システムについて議論する。システムのユーザである視覚障害者は携帯型の端末を持ち、無線通信を介して支援情報を取得する。携帯端末は、支援情報を音声や振動などの形態で再生する。センサノードは、センサと計算機から構成され、センサの出力信号を情報処理してユーザに有用な動的情報を生成する。

各センサノードは、お互いに一定の距離をおいて設置される。このようにすることで、すべてのセンサノードが局所的な温度の上昇や電磁ノイズの影響を同時に受ける可能性を低減することができる。提案手法を適用したシステム

では, 3個のセンサノード  $S_1, S_2, S_3$  を1組として設置する。3個のセンサノードは同一の地点を監視し, 多数決によって誤りのマスクを行う。

センサノード同士は有線LANで接続する。この有線LANは, センサノード同士の通信に専用として用いる。有線LANはルータを含まず, 必要に応じてリピータだけを含む。このため, 有線LANを介したセンサノード同士の通信では, 通信遅延の上限  $D$  を定数として見積もることができる。

3個のセンサノードは, 有線LANを介して時刻同期アルゴリズムを実行し, 緩やかに時計を同期する。本研究では, インターネット上の時刻同期プロトコルとして広く利用されているNTP<sup>(7)</sup>を用いた。ここで, ある時点における各センサノードの時刻の差の最大値が, 平均して定数  $\delta$  であると仮定する。通常,  $\delta$  は約  $500\mu\text{s}$  程度と考えられる。

図2にセンサノードの分散アルゴリズムを示す。センサノードは一定時間  $T_S$  ごとにセンシングと情報処理を行う。この時間間隔  $T_S$  をセンシング間隔と呼ぶ。センサノード  $S_i$  は, 時刻  $t$  におけるセンサ出力の情報処理を終えると, 処理の結果  $x_{t,i}$  とタイムスタンプ  $t$  を含む情報メッセージ  $M_{t,i}$  を他ノードに送信する。情報メッセージを受信したノードは, 時刻  $t$  の結果  $x_{t,k}$  ( $k=1, 2, 3$ ) のうち2つ以上を保持していれば多数決を行い, 結果として  $v_t \equiv \text{maj}(x_{t,1}, x_{t,2}, x_{t,3})$  を得る。ここで,  $\text{maj}(\cdot)$  は多数決関数であり,  $x_{t,1}, x_{t,2}, x_{t,3}$  の値のうち過半数を占めるものを与える。多数決が成功した場合,  $S_i$  が保持しているすべての  $x_{t,k}$  と  $v_t$ , および時刻  $t$  を含む情報メッセージを生成し, ユーザの携帯端末に送信する。

各センサノードは, 一定時間  $T_H$  ごとにハートビートと呼ばれるメッセージを他のセンサノードに送信する。各ノードは, どのノードが故障と考えられるかを示す集合  $\text{SUSPECT}$  を管理する。センサノード  $S_i$  ( $i=1, 2, 3$ ) は,  $S_j$  ( $i \neq j$ ) から  $l$  番目のハートビート  $H_l$  を受信後,  $T+D+\delta$  時間以内に次のハートビート  $H_{l+1}$  を受信できなければ,  $S_j$  が故障しているものとみなし,  $\text{SUSPECT}$  に  $S_j$  を追加する。また,  $S_i$  が保持するすべての  $x_{t,k}$  と時刻  $t$  を含む情報メッセージを生

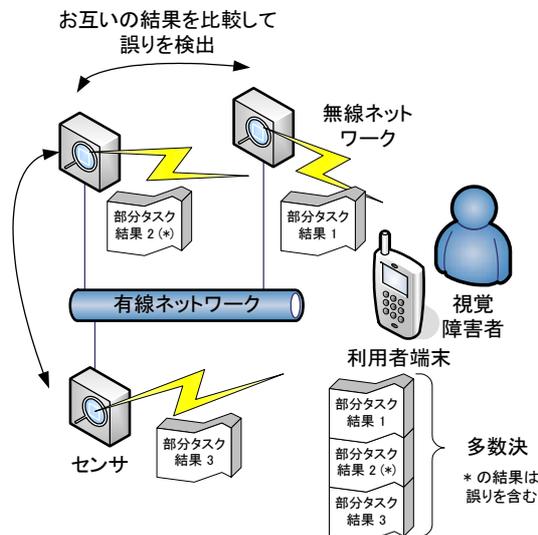


図1. 視覚障害者移動支援システムの構成

```

t = 0; /* local clock value */
SURVIV = ∅ ; SUSPECT = {S1, S2, S3};
X(·) = ∅ ;

vote(τ) {
  if (|X(τ)| < 2) return false;
  if (|X(τ)| = 2)
    if (x_{τ,i}=x_{τ,j} | x_{τ,i}, x_{τ,j} ∈ X(τ)) { v_τ = x_{τ,i}; return true; }
    else return false;
  if (x_{τ,1} = x_{τ,2} or x_{τ,2} = x_{τ,3} or x_{τ,3} = x_{τ,1})
    { v_τ = maj(x_{τ,1}, x_{τ,2}, x_{τ,3}); return true; }
  return false;
}

every T_S {
  t = t+1;
  y = sensor output;
  x_{t,myid} = process_sensor_output(y);
  X(t) = X(t) ∪ x_{t,myid};
  if (vote(t)) M = information_message(t, X(t), v_t);
  else M = information_message(t, X(t));
  send M to other sensor nodes;
}

every T_H {
  send heartbeat to other sensor nodes;
  SUSPECT = {S1, S2, S3} - SURVIV;
  SURVIV = ∅ ;
  if (!vote(X(t))) {
    M = information_message(t, X(t));
    send M to user terminal;
  }
}

on receiving information message M_{t,k} {
  X(τ) = X(τ) ∪ x_{τ,j} (x_{τ,j} ∈ X(τ) in M_{t,k});
  if (vote(τ)) {
    M = information_message(τ, X(τ), v_τ);
    send M to user terminal;
  }
}

on receiving heartbeat from S_j { SURVIV = SURVIV ∪ S_j;

```

図2. センサノードの分散アルゴリズム

```

X(·) = ∅ ;
on receiving information message M_{t,k} {
  for each x_{t,j} included in M_{t,k} { X(t) = (X(t) ∪ x_{t,j}) }
  v = vote(t);
  if ((vote failed) or (M_{t,k} has v_t and v ≠ v_t))
    warn user on a system trouble;
  else if (v means dangerous)
    warn user of a danger;
}

```

図3. ユーザ端末の多数決アルゴリズム

成し、携帯端末に送信する。センサノードにおいて、これらのアルゴリズムの実行に要する時間を  $T_V$  とする。

携帯端末がセンサノードと通信可能な位置まで近づくと、情報メッセージが受信される。携帯端末は、 $L$  個の情報メッセージ  $M_{(L-1),k}, M_{(L-2),k}, \dots, M_{0,k}$  を受信し、これらの到着間隔の最大値  $T_W$  を求める。以後の通信では、 $T_W$  を平均的な無線通信遅延と見なし、これを用いて障害の検知を行う。

ユーザの携帯端末が定常状態で実行する多数決アルゴリズムを図3に示す。携帯端末は、情報メッセージ  $M_{i,k}$  を2つ以上受信するとこれらの中で多数決を行う。 $M_{i,k}$  がセンサノードによる多数決の結果値  $v_i$  を含んでいる場合は、自身の多数決結果と  $v_i$  が一致することを確認し、不一致の場合ユーザに警告を行う。また、 $M_{i-1,k}$  の受信後、 $\alpha T_W$  時間待っても  $v_i$  を含む情報メッセージが受信されない場合、障害が発生したと見なしユーザに警告を行う。ただし、 $\alpha$  は定数とする。提案手法は、表1のような障害に対して、サービスの継続、またはユーザへの警告を行うことができる。

#### 4. 数値例と考察

提案アルゴリズムを市販の組込み Linux 機と PDA を用いて試験的に実装した。実装には C++ 言語を用いた。センサノードは、ハートビートと情報メッセージの2種のメッセージを扱うが、これらを統合して1つのメッセージにまとめることで、ネットワーク帯域の効率的な利用が可能である。試験実装では、センシング間隔  $T_S$  を十分短くすることで、情報メッセージにハートビートの役割を兼ねさせた。

試験実装システムの1つのセンサノードに意図的に誤りを挿入し、これをマスクできることを確認した。また、ネットワーク・エミュレータを用いて通信遅延を発生させ、携帯端末が警告を発することを確認した。

図4は、高々1つのセンサノードに誤りが発生する場合において、ユーザ端末に多数決結果  $v_i$  を含む情報メッセージが受信されるまでの所要時間を示している。横軸は、センシング間隔  $T_S (=T_H)$  を示す。図から多数決による遅延は、 $T_S$  が非常に短い、または長い場合に大きくなるのが分かる。 $T_S = 1$  のとき、最大所要時間は150ms程度である。ユーザの歩行速度を5km/hとし、センサノードにおける情報処理に500ms必要であると仮定すると、これらの合計時間の間にユーザが進む距離は約1mである。このことから、試験

表1. 提案手法の障害への対応

障害または誤り	対応
1つ以下のセンサノードの故障停止または誤り	多数決によって $T_V + D$ 時間で訂正できる
2つ以上のセンサノードの誤り	多数決によって $T_V + D$ 時間で誤りを検出し、警告できる
2つ以上のセンサノードの故障停止	$T_H + D$ 時間で検出し、警告できる
有線 LAN の障害	$T_H + D$ 時間で検出し、警告できる
無線 LAN の障害	$\alpha T_W$ 時間で検出し、警告できる

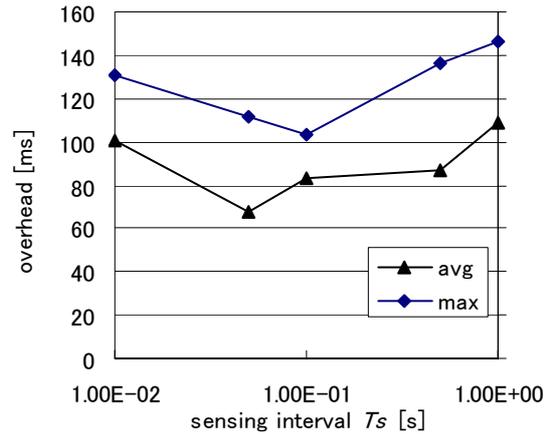


図4. 試験実装の多数決所要時間

高々1つのセンサノードに誤りが生じる際の多数決所要時間の平均と最大値 ( $T_S = T_H$ ,  $T_V = 50\text{ms}$ ,  $D = 50\text{ms}$ ,  $\delta = 500\mu\text{s}$ ,  $\alpha = 2$ )

実装は、歩行者支援に十分な応答性を持つと考えられる。

#### 5. まとめ

本研究では、視覚障害者移動支援システムを高信頼化する分散多数決冗長手法を提案し、試験実装を行った。実験の結果、提案手法は多数決によって単一の誤りをマスクできること、通信遅延が発生した際にも安全側に処理を移せることが確認された。また、多数決の所要時間は歩行速度に比べて十分短いことが確かめられた。

提案手法において、ユーザの持つ携帯型端末は、単一故障発生点 (single point of failure) となりうる。すなわち、センサノードは冗長化によって故障に耐えられるが、携帯端末が故障するとそのユーザはサービスを受けられない。これは、ユーザが特別な装置を持つ必要があるシステムの本質的な問題であると考えられる。環境側にスピーカを設置し音声情報を再生するなどの方法を併用することで改善できる可能性があるが、これは今後の課題である。

(平成18年10月25日受付, 平成18年12月4日再受付)

#### 文 献

- (1) 米田友洋, 梶原誠司, 土屋達弘: ディペンダブルシステム, オーム社 (2005)
- (2) Fischer, et al.: "Impossibility of Distributed Consensus with One Faulty Process," J. ACM, Vol.32, No.2 pp.374-382 (1985)
- (3) A. Hopkins, T. Smith, J. Lala: "FTMP—A Highly Reliable Fault Tolerant Multiprocessor for Aircraft," Proc. IEEE, Vol.66, No.10 pp.1221-1239 (1978)
- (4) J. H. Wensley, L. Lamport, J. Goldberg, M. W. Green, K. N. Levitt, P. M. Melliar-Smith, R. E. Shostak, and C. B. Weinstock: "SIFT: Design and Analysis of a Fault-Tolerant Computer for Aircraft Control," Proc. IEEE, Vol.66, No.10 pp.1240-1255 (1978)
- (5) D. K. Pradhan and N. H. Vaidya: "Roll-Forward Checkpointing Scheme: A Novel Fault-Tolerant Architecture," IEEE Trans. Comput., Vol.43, No.10 pp.1163-1174 (1994)
- (6) 大原衛, 新井雅之, 福本聡, 岩崎一彦: 「部分再試行による多数決冗長方式」, 電子情報通信学会技術研究報告, DC2003-102, pp. 73-78 (2004)
- (7) D. L. Mills: "Network Time Protocol (Version 3) Specification, Implementation and Analysis," RFC1305 (1992)