6K-04

# ビザンチンエージェントが混在するモバイルエージェント群による乱択集合アルゴリズム *

小杉泰雅 †　　首藤裕一 ‡

法政大学 情報科学部

## 1　はじめに

$n$ 頂点からなる無向連結グラフ上の頂点に任意に配置された $k$ 体のモバイルエージェント（以下、エージェント）をひとつの頂点に集める**集合問題**を考える。エージェントはグラフの辺を移動することで頂点間を自由に移動できる。エージェントは一意な識別子（以下、ID）を持つが、グラフ上の頂点に ID は存在しない。頂点に ID が存在すると、ID が最小の頂点にすべてのエージェントが移動することで集合問題が容易に解けるからである。

本研究では、アルゴリズムに従わず、任意の敵対的な動作をする $f$ $(\leq k-1)$ 体のエージェント (以下、**ビザンチンエージェント**) がエージェント群に混在したときの集合問題について考える。当然ながら、ビザンチンエージェントが混在する場合は、すべてのエージェントをひとつの頂点に集合させることはできない。そこで、問題の定義をわずかに緩める。具体的には、すべての非ビザンチンエージェント (以下、**正常エージェント**) が一つの頂点に集合すればよいとする。

## 2　土田ら [2] のアルゴリズム

この問題に関する研究はいくつか存在するが、ここでは本研究に最も関連する土田ら [2] の研究を紹介する。土田ら [2] は、**認証付き白板**と呼ばれる、各エージェントが自由に読み書き可能な頂点上のメモリを用いることで、ビザンチンエージェントが混在するエージェント群の集合を高速に実現するアルゴリズムを提案した。各頂点の認証付き白板には、エージェントごとに専用の読み書き領域が用意されており、各エージェントは、他のエージェントの領域の内容を読むことはできるが、更新することはできない。また、各エージェントは署名機能を具備していることを仮定する。すなわち、各エージェントは、任意の文字列に対して、自身の ID に紐付いた公開鍵で検証可能な署名を付与できる。このアルゴリズムは、$f \leq F$ を満たす整数 $F$ が全エージェントに共有されているという仮定のもと、同期的に動作を行うモバイルエージェント群を一つの頂点に $O(Fm)$ 時間で集合させることを保証する。ここで、$m$ はグラフの辺の数である。集合にあたって必要な正常エージェント数に制限はない。

紙面の都合上、署名機能の詳細な説明は割愛するが、この仮定はビザンチンエージェントの行動を制限するうえで極めて有効である。具体的には、エージェント間の情報のやり取りに署名をつけることをアルゴリズムとして強制することで、ビザンチンエージェント $b$ は、自身のビザンチン性を露呈することなく相異なる 2 つの正常エージェント $a_A, a_B$ に整合性の取れない偽情報 $A, B$ を流すことができなくなる。というのは、$A$ および $B$ には $b$ の署名をつけておく必要があり（そうでないと $a_A, a_B$ は $A$ および $B$ を無視する）、$a_A$ と $a_B$ はそれぞれ $b$ の署名付き情報 $A$ と $B$ をすべての頂点の白板に書き込むことで、不整合が生じる情報 $A$ と $B$ を白板に書き込んだこと、すなわち、$b$ がビザンチンエージェントであることをすべての正常エージェントに証明することができる。

## 3　本研究の成果

本研究では、土田ら [2] と同様に認証付き白板は用いるものの、各エージェントが乱数を利用できるという仮定をおくことで、署名機能を必要としないアルゴリズムを与える。ただし、引き続き、各エージェントは白板に書き込まれた各情報がどのエージェントによって書き込まれたのかは認識することができるものとする。また、土田らのアルゴリズムがビザンチンエージェント数 $f$ の上界 $F$ の知識を仮定していたのに対し、本アルゴリズ

---

* Byzantine-tolerant randomized gathering

† Taiga Kosugi, Hosei University

‡ Yuichi Sudo, Hosei University

表1　ビザンチンエージェントが混在する環境での集合アルゴリズム

| | 初期知識 | ビザンチン数の条件 | 白板 | 署名機能 | 時間計算量 | 成功確率 |
|---|---|---|---|---|---|---|
| [1] | $k \leq n \leq N$ | なし | なし | なし | $O(N^9 \lambda \log N)$ | 1 |
| [2] | $f \leq F$ | なし | あり | あり | $O(Fm)$ | 1 |
| 本研究 | $k \leq K, \lambda \leq \Lambda$ | なし | あり | なし | $O(m + (\alpha + \log K)nK\Lambda)$ | $1 - 2^{-\alpha}$ |

**Algorithm 1:** 提案アルゴリズム

```
1 深さ優先探索を行いトポロジを把握
2 for h = 1 to ((α + log)K))K do
3 |   b ← SelectTarget()
4 |   GoToTarget(b)
5 終了を宣言
```

ムはエージェント数 $k$ の上界 $K$ と、エージェントの最大 $ID$ 長である $\lambda$ の上界 $\Lambda$ の知識を仮定する。このアルゴリズムはデザインパラメータとして任意の整数 $\alpha$ を取る。時間計算量は $O(m + (\alpha + \log K)nK\Lambda)$ であり、アルゴリズム停止時に集合が解けている確率は $1 - 1/2^{\alpha}$ である。ここで、$\lambda$ はエージェント ID の最大ビット長である。なお、本稿では混乱が生じない限りエージェント $a$ とその ID を混用して記述する。

## 4　提案アルゴリズム

提案アルゴリズムの擬似コードを Algorithm 1 に示す。各正常エージェント $a_i$ は前処理として $2m$ ラウンドをかけて深さ優先探索を行い、グラフのトポロジを把握する。トポロジの把握により、以後、いつでも全頂点を $2n-2$ ラウンドで訪問することができる。また、このときに $a_i$ は全頂点の白板に訪問済みの印をつけておく。こうすることで、各エージェント $a_i$ は任意の時刻 $t$ において、現在地の白板に印をつけているエージェントの ID を確認することで、現在地に滞在しているすべてのエージェントとのあいだで、正常エージェントの集合の上位集合となるエージェントの集合 $T_{i,t}$ を共有することができる。その後、関数 SelectTarget() と GoToTarget() をちょうど $(\alpha + \log K)K$ 回繰り返してアルゴリズムを停止する。

SelectTarget() と GoToTarget() について簡単に説明する。SelectTarget() は 1 ラウンドで完了する関数であり、時刻 $t$ で $a_i$ と同じ頂点 $v$ に滞在しているすべてのエージェント全員（この集合を $A_{i,t}$ とする）で共通のエージェントを標的として選択する。この標的は、$T_{i,t}$ のなかから等確率に選択される。この処理は、時刻 $t$ で $A_{i,t}$ 中の各エージェント $a$ が $[0, |T_{i,t}| - 1]$ の範囲で整数 $r_a$ を等確率に選択して白板 $v$ に書き込み、時刻 $t+1$ で $j = \sum_{a \in A_{i,t}} r_a \bmod |T_{i,t}|$ を計算し、$T_{i,t}$ のなかで ID が $j$ 番目に小さなエージェントを選択することで実現できる。GoToTarget($b$) は $O(\lambda n)$ ラウンドで完了する関数であり、標的 $b$ への合流を試みる。紙面の都合上詳細は割愛するが、GoToTarget($b$) は以下の 2 点を保証する。

- GoToTarget($b$) 開始時に $a_i$ と同じ頂点にいた正常エージェントは、GoToTarget($b$) 終了時にも $a_i$ と同じ頂点にいる。
- 標的 $b$ が正常であれば、GoToTarget($b$) 終了時に $a_i$ と $b$ は同じ頂点にいる。

アルゴリズム終了時に確率 $1 - 2^{-\alpha}$ 以上で集合問題が解けていることを示す。いま、$a_i$ を任意の正常エージェントとする。アルゴリズムのつくりから、$a_i$ が高々 $k$ 体存在するすべての正常エージェントをそれぞれ少なくとも 1 回標的として選択し、GoToTarget() を実行すれば集合は達成される。任意の時刻 $t$ について $|T_{i,t}| \leq k$ であるから、その確率は少なくとも $1 - k(1 - 1/k)^{(\alpha + \log K)K} \geq 1 - 2^{-\alpha}$ である。

## 参考文献


[1] Y. Dieudonné, A. Pelc, and D. Peleg. Gathering despite mischief. *ACM Transactions on Algorithms (TALG)*, 11(1):1–28, 2014.

[2] M. Tsuchida, F. Ooshita, and M. Inoue. Gathering of mobile agents in asynchronous byzantine environments with authenticated whiteboards. In *International Conference on Networked Systems*, pages 85–99. Springer, 2018.