4ZC-01

リスト管理手法を用いたエクスターナルグリッドにおける信頼性の定量的評価

伊賀 俊輔 † 遠藤 慶一 ‡ 小林 真也 ‡
愛媛大学工学部工学科 † 愛媛大学大学院理工学研究科 ‡

1 研究背景

ネットワーク上の計算機を用い分散処理を行うことで，高い処理能力や記憶容量を得る技術をグリッドコンピューティングという．グリッドコンピューティングは，インターナルグリッドとエクスターナルグリッドに分類される．インターナルグリッドは，イントラネット上の計算機を用いるため，比較的安全であるが，接続可能台数が限られているため高い処理能力が期待できない．一方，エクスターナルグリッドは，インターネット上の計算機を用いるため，実質的に無限台の計算機を利用でき，高い処理能力が期待できるが，悪意を持った人物の計算機が紛れ込み，不正行為を働く可能性がある．

1.1 悪人による不正行為

悪意を持った計算機のことを悪人，正常な処理を行う計算機を善人と呼ぶ．悪人は，間者と改竄者，怠業者に分類される．間者は，善人のように振る舞うが，プログラムの内容やデータを盗み取り，不正な解析を行う計算機である．改竄者は，意図的に誤った結果を返し，正常な処理を妨害する計算機である．怠業者は，正しい処理を行うが，意図的に結果を返すまでの時間を遅らせることで，全体の処理の遅延を目論む．

1.2 セキュアプロセッシング

不正な解析への対策としてプログラム分割，不正な改竄への対策として処理の多重化が挙げられる．

1.2.1 プログラム分割

処理ノードに依頼するプログラムを複数の断片に分割し，各断片を別々の処理ノードへ依頼することで，1つの処理ノードが得られる情報量を制限することができ，依頼したノードが間者の場合でも間者が得る情報量を削減できる．

1.2.2 処理の多重化

処理の多重化は，1つの処理を複数の処理ノードに依頼する．依頼した処理ノードから返された結果に対して多数決処理を行うことで採用する結果を確定する．これにより，改竄者によって改竄された結果が混入していてもその数が過半数未満であれば，正しい結果を採用することができる．同一の処理を行う処理ノードの数を多重度といい，結果を採用するために必要な同一の処理結果の数を確定閾値という．

処理の多重化は，確定閾値と同数の結果が得られるまで結果の確定を待つ必要があるため，高速な処理ノードがグリッド内に存在していても，その性能を活かしきれない．

1.2.3 先行処理手法

処理の多重化における処理時間増加の問題に対して，先行処理手法が提案された [1]．先行処理手法は，確定閾値と同数の処理結果が揃うまで待たず，早く結果を返した処理ノードの結果を暫定的な結果として，次の処理を先行して開始する手法である．多数決処理の結果が暫定的な結果と一致すれば，継続して処理を進め，一致しない場合は先行していた処理を中止し，多数決によって確定した結果を用いて処理をやり直す．このやり直し処理をロールバックという．

改竄者の割合が大きくなれば，暫定的な結果と多数決処理による結果が異なる確率が大きくなり，ロールバックの頻度が増加し，結果として処理時間が増加するという問題がある．

1.2.4 リスト管理手法

先行処理手法の問題に対して，真正な処理結果のみを返す，かつ高速な処理ノードをリスト管理し，リストから複数の処理ノードを選択することで信頼性の向上と処理時間の短縮を行うリスト管理手法が提案された．正しい結果を返し，かつ高速な処理ノードはホワイトリスト，正しい結果を返すが，低速な処理ノードはブルーリスト，誤った結果を返す処理ノードをブラックリストで管理する．これまでに，リスト管理手法を用いたエクスターナルグリッドにおける機密性と高速性については定量的評価を行った．しかし，処理結果の正しさである信頼性については定量的評価がされていない．

1.3 研究目的・目標

リスト管理手法を用いたエクスターナルグリッドにおいて，信頼性の観点からリスト管理手法の有効性を示す．また，リスト管理手法を用いたエクスターナルグリッドの信頼性を定量的に評価し，リスト管理手法を用いない場合と比較・考察を行う．

2 評価手法

2.1 信頼性評価における条件

改竄者は結託し1つの集団を形成すると仮定する．改竄者が結託すると，改竄された同一の処理結果を返し，誤った結果が採用される確率を高くすることができ，危険性が増す．より改竄が起こりやすい，この条件下での評価を行う．

Quantitative Evaluation of Reliability in External Grids Using List-based Node Management Method

† S. Iga
Department of Engineering, Faculty of Engineering, Ehime University
‡ K. Endo, S. Kobayashi
Graduate School of Science and Engineering, Ehime University

表 1　信頼性を求める際の設定条件

多重度 m	30
インターネット上の改竄者の存在確率 $P_{vr} + P_{vw}$	0.0 ～ 0.25
ホワイトリストから選択する数 n	0 ～ $\lceil \frac{m-1}{2} \rceil$
インターネット上の処理ノードの故障率 P_{wrong}	0.01
ホワイトリスト内の処理ノードの故障率 P_{Lwrong}	0.01
プログラム分割数 D	100

全ての処理ノードは故障を起こす可能性があるが，ホワイトリスト内の処理ノードの故障率はインターネット上の計算機の故障率以下であると考える．これは，ホワイトリスト内の計算機は，ある時点では正しい処理を行ったことが保証されるが，インターネット上の計算機は過去の状態について未知であるためである．

ホワイトリスト内に紛れ込んだ改竄者の存在確率は，インターネット上の改竄者の存在確率よりも低いことが想定される．これは，ホワイトリストに紛れる改竄者は，過去に正しい結果を高速で返しており，実績のない計算機に比べ信用できると考えられるためである．しかし，実際にどの程度改竄者がホワイトリストに潜入しているかが不明である．ここでは，インターネット内の改竄者の存在割合に対する，ホワイトリスト内の改善者の存在割合の比 R(式 (1)) を定め，R の値の違いによる影響について評価する．

$$R = \frac{\text{ホワイトリスト内の改竄者の存在確率}}{\text{インターネット上の改竄者の存在確率}} \tag{1}$$

2.2　信頼性の評価式

多重度 m が奇数の場合，インターネット上の故障していない改竄者の存在確率を P_{vr}，ホワイトリスト内の故障していない改竄者の存在確率を P_{lvr}，ホワイトリストから選択する処理ノード数を n とすると，プログラム断片が正しくない確率 P_{lof} は式 (2) となる．

$$P_{lof} = \sum_{j=0}^{n} \left\{ {}_nC_j {P_{lvr}}^j (1-P_{lvr})^{n-j} \sum_{k=\frac{m+1}{2}-j}^{m-n} {}_{m-n}C_k {P_{vr}}^k (1-P_{vr})^{m-n-k} \right\} \tag{2}$$

多重度 m が奇数の場合，インターネット上の故障していない善人の存在確率を P_{gr}，ホワイトリスト内の故障していない善人の存在確率を P_{lgr}，ホワイトリストから選択する処理ノード数を n とすると，プログラム断片が正しい確率 P_{lof} は式 (3) となる．

$$P_{lot} = \sum_{i=0}^{n} \left\{ {}_nC_i {P_{lr}}^i (1-P_{lr})^{n-i} \sum_{k=\frac{m+1}{2}-i}^{m-n} {}_{m-n}C_k {P_{gr}}^k (1-P_{gr})^{m-n-k} \right\} \tag{3}$$

票割れが起こったとしても，全体の処理を通して P_{lof} と P_{lot} の比率は一定であるため，多重度が奇数の場合，プログラム断片が票割れを起こしても正しい確率 P_{LO} は式 (4) となる．

$$P_{LO} = \frac{P_{lot}}{P_{lof} + P_{lot}} \tag{4}$$

多重度が偶数の場合は，確定閾値が変化するだけなので省略する．

また，プログラム全体が正しい確率 P_d は，プログラム分割数 D を用いると式 (5) となる．

$$P_d = {P_{LO}}^D \tag{5}$$

3　結果・考察

今回の実験で設定した条件を表 1 に示す．図 1 は，インターネット上の改竄者の存在確率とホワイトリストから選択する処理ノードの数 n を変化させた際の信頼性のグラフである．$n = 0$ はリスト管理手法を用いない場合を示しており，n が大きくなるほど信頼性が高くなることから，信頼性の観点ではリスト管理手法は有効であるといえる．また，インターネット上の改竄者の存在確率が 0.05 の場合は，n の値に関係なくプログラム全体が正しく処理される確率が，0.9999999999 以上，いわゆるテン・ナインを満たしている．これは，リスト管理手法の有無に関係なく要件を満たしていることから，多重度が影響していると考える．多重度が 30 の場合，リスト管理手法を最大限利用すると，インターネット上の改竄者の存在確率が 0.125 まではテン・ナインを保証できる．

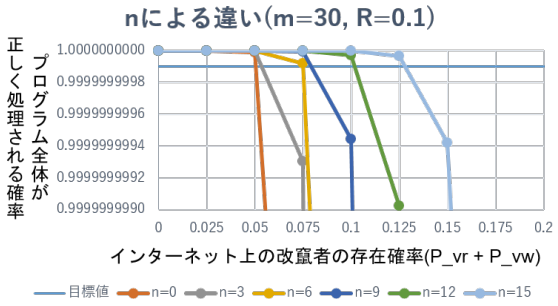

図 1　n を変化のときの信頼性の変化

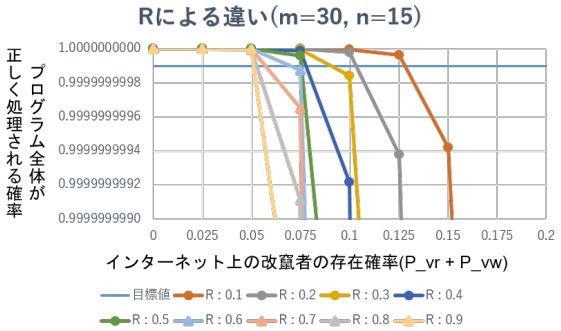

図 2　R を変化させたときの信頼性の変化

図 2 は，インターネット上の改竄者の存在確率と R の値を変化させた際の信頼性のグラフである．信頼性は R の値が小さいほど高くなる．また，$R = 0.9$ の場合でもインターネット上の改竄者の存在確率が 0.05 程度であれば，テン・ナインを満たすことができる．

4　おわりに

今後の課題として，ブルーリストを活用した場合に，どの程度の改竄者の存在確率までテン・ナインを満たすかの検証と高速性・機密性とのトレードオフ関係の検証が挙げられる．

参考文献

[1] 大西 伊吹，遠藤 慶一，小林 真也，” エクスターナルグリッドにおける各種先行処理手法の定量的比較”，情報処理学会第 82 回全国大会講演論文集 (4)，pp.141-142，2020.