5V-05

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

大西 伊吹 † 遠藤 慶一 ‡ 小林 真也 ‡
愛媛大学工学部情報工学科 † 愛媛大学大学院理工学研究科 ‡

1. はじめに

グリッドコンピューティングとはネットワーク上に存在する計算資源を統合し，分散処理することで，高性能な処理能力を得ることのできる技術である．グリッドコンピューティングの一種であるエクスターナルグリッドは，インターネット上に存在する不特定多数の計算機でグリッドを構成するため，悪意を持った人間の所有する計算機 (以下悪人という) であれば，不正行為を働く可能性がある．

不正行為には，処理内容が不正に取得されることによる「処理内容の漏洩」と，処理の委託先が正しい結果を返さないことによる「処理結果の改竄」が考えられる．これらの問題を解決するため，セキュアプロセッシングの研究が行われてきた．しかし，セキュアプロセッシングは，処理速度の低下を伴う．この問題に対しては，先行処理という手法の研究が行われている．

先行処理には，網羅法，閾値網羅法，閾値暫定法の三種類の手法があるが，それぞれ，処理内容の漏洩への耐性 (機密性)，処理結果の改竄に対する耐性 (信頼性)，処理速度性能 (高速性) が異なる．しかし，現状ではそれらの定量的な比較は行われていない．

本研究では，先行処理の三種の手法を機密性，信頼性，高速性の観点から定量的に比較し，グリッド管理者が処理目的に合わせた先行処理手法を選択できるようにすることを目指す．

2. セキュアプロセッシング

2.1. プログラム分割

プログラム分割は，処理内容の漏洩への対策である．依頼するプログラムを複数のプログラム (以下，プログラム断片と呼ぶ) に分割し，異なる計算機に処理を依頼する．これにより，委託するプログラム一つあたりの情報量を減らし，不正な解析を抑制することができる．

2.2. 処理の多重化

処理の多重化は，処理結果の改竄への対策である．処理を一つのノードに依頼するのではなく，複数のノードへ同一の処理を依頼し，その処理結果を多数決により確定することで，信頼性を確保することができる．

同一の処理を依頼するノードの中に，虚偽の結果を返してくるノードが存在しても，他の正しい結果を返すノードにより，多数決後の結果は正しい結果となる．

同一の処理を行う処理ノードの台数を,「多重度」という．

3. 先行処理

処理の多重化は，計算機を複数使用して多数決を行うため，処理ノードの性能差により投票待ちが発生する．これは，信頼性を向上させるというメリットの一方で，処理時間が増加してしまうというデメリットが有る．このデメリットを解決するため，多重化において，多数決が終了する前に暫定的に次の処理を開始する先行処理という手法が提案されている．

先行処理には，網羅法，閾値暫定法，閾値網羅法の 3 つが存在する．

3.1. 網羅法

この手法では，処理を依頼したノードが返した結果のうち，先行処理をまだ開始していない結果全てに対して並列に先行処理を行う方法である．

高速な処理が期待できる反面，参加する処理ノードの数が非常に多くなるため，プログラム断片を不正に取得される可能性が高くなる．

3.2. 閾値網羅法

この手法では，処理を依頼したノードが返した結果のうち，一定数同じ結果が返ってきたもの全てに対して並列に先行処理を行う方法である．この一定数のことを暫定閾値と呼ぶ．

網羅法での過剰な処理ノードの参加を抑える狙いがある．

3.3. 閾値暫定法

この手法では，処理を依頼したノードが返した結果のうち，最も早く暫定閾値と等しい数の結果が返ってきた 1 つのみを先行処理する方法である．

閾値網羅法以上に参加するノード数を抑えることができるが，先行処理の結果が最終的な多数決の結果とは違っていた場合は，処理速度を向上させる効果が無い．

4. 各指標の概念

本研究で定量的な評価を行う対象は，処理の多重化，プログラム分割，先行処理を取り入れたエクスターナルグリッドである．また，グリッドに参加した悪人は，全員が不正確な同一の結果を返し，処理結果を改ざんしようとするものとする．

シミュレーションを行う際の計算機の処理性能は，形状尺度 $k = 5$，尺度分母$\theta = 2/5$，期待値 2 のガンマ分布に基づくものとする．

4.1. 信頼性

プログラム全体の結果が正しくなる確率は, 全ての部分プログラムが正しい結果を返す確率と等しい．

ある部分プログラム a が正しい結果を返す確率 P_a は, 式 (1) で表せる．ただし, 式中の p は処理ノードが正しい結果を返す確率 (真正処理率),m は多重度,V_k は多

Quantitative comparison of various advanced processing methods in the external grid
I. Oonishi, Department of Computer Science, Faculty of Engineering, Ehime University
K. Endo, S. Kobayashi, Graduate School of Science and Engineering, Ehime University

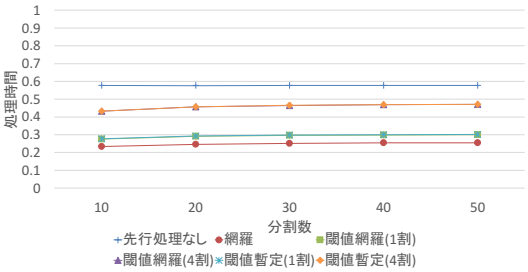

図 1: 分割数を変化させた場合の高速性の変化 (悪人の存在確率 5%)

数決結果が確定する値 (確定閾値) とする.

$$P_a = \sum_{n=0}^{m-V_k} {}_mC_{m-n} p^{m-n}(1-p)^n \tag{1}$$

プログラム分割数を n とするとき, プログラム全体の結果が正しくなる確率 P は,

$$P = P_a^n \tag{2}$$

と表せる.

この P を, 信頼性の定量的評価の指標として用いる.

4.2. 高速性

グリッドが処理を開始してから，プログラム全体の処理の終了までにかかった時間を，定量的評価の指標に用いる．このとき，通信によるオーバーヘッドは，先行処理手法やパラメータの違いによって変化せず，環境への依存度も高いことから考慮しないこととする．

4.3. 機密性

プログラム全体のうち悪人に取得されたプログラム断片の割合，取得されたプログラム断片群の数，最大保護連続長，最大被取得連続長を，定量的評価の指標に用いる．

5. 結果と考察

信頼性に関しては，4.1 の式 (2) の結果が，先行処理手法によって変化しないため，信頼性が先行処理手法の種類によっては変化しないことがわかる．

図 1 は分割数を変化させた際のプログラムの処理時間の変化のグラフである．このグラフから，高速性に関してプログラム分割数，多重度，悪人の存在確率を変化させても，プログラムの処理時間に大きな変化はなく，網羅法，閾値網羅法 (1 割) と閾値暫定法 (1 割)，閾値網羅法 (4 割) と閾値暫定法 (4 割)，先行処理なしの順に処理時間が短い結果が読み取れる．

図 2 と図 3 は，分割数を変化させた際のプログラム断片の被取得割合の変化のグラフである．機密性に関して，プログラム分割の変化は，機密性に大きな影響は与えなかった．

悪人の存在確率において，先行処理なしの場合ではプログラム断片の被取得割合は変化しないが，閾値網羅法 (1 割)，閾値暫定法 (1,4 割) においては，5%の際は先行処理なしとほぼ同等の被取得割合なのに対し，10%の際は 90%近くになっている．

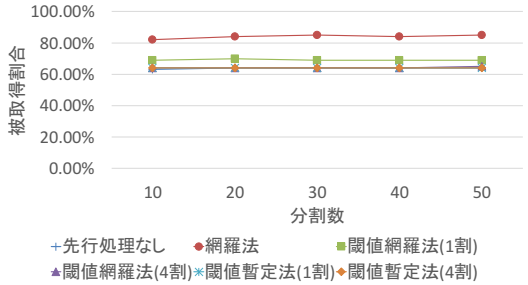

図 2: 分割数を変化させた場合の被取得割合の変化 (悪人の存在確率 5%)

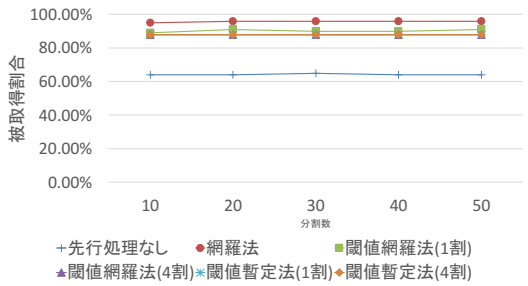

図 3: 分割数を変化させた場合の被取得割合の変化 (悪人の存在確率 10%)

これらの結果より，処理速度を重視する際は網羅法の利用が，機密性を重視する場合は，暫定閾値の低い値の閾値暫定法を利用することが望ましいと言える．ただし，閾値暫定法は，悪人の存在確率の小さな変化が機密性の大きな低下を招くため，多くの悪人の存在が懸念される場合は，機密性を損なわないために先行処理を行わないほうが良いと考えられる．

6. まとめ

本稿では，エクスターナルグリッドにおける各先行処理手法の高速性と機密性を比較した．

高速性では条件による処理速度の変化は見られず，機密性では悪人の存在確率においてのみ取得されたプログラム断片の割合が変化した．このことから，想定される悪人の存在確率と，望まれる処理速度のみを焦点として先行処理手法を決定すれば良い事がわかる．今後の課題として，暫定閾値が高い場合の閾値網羅法と閾値暫定法における高速性と機密性についての詳細な比較が挙げられる．

参考文献

[1] 田中祐生 遠藤慶一 樋上喜信 小林真也 (2017) ”閾値暫定法を用いたエクスターナルグリッドにおける高速性・機密性・信頼性のトレードオフ関係の定量的考察” 情報処理学会第 79 回全国大会講演論文集