6S-06

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

田中祐生† 遠藤慶一‡ 樋上喜信‡ 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，分散処理をすることで，高性能な処理能力を得ることができる技術である．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，悪意をも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．そのため，エクスターナルグリッドは商用目的での実用化がされていない．実用化を阻害する要因として，処理が第三者にあからさまになる危険性がある，という “処理の隠蔽” に関する問題と，処理の委託先が本当に正しく処理結果を返答してくるのか，という “処理の委託に対する信用性確保” の問題がある．これらの問題を解決すべく，これまで，セキュアプロセッシングの研究を行ってきた [1]．しかし，セキュアプロセッシングを用いると，処理時間が増加してしまうという，高速性についての問題が新たに発生した．この問題に対しては，先行処理という手法の研究を行っている．

エクスターナルグリッドを実用化させるには，機密性や信頼性が確保されなければならない．そのため，本研究では，解析的な手法や，シミュレーションにより，高速性・機密性・信頼性の定量的な評価を行い，これらの指標のトレードオフの関係性を示す．

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，“処理の隠蔽の問題” に対する解決策である．依頼するプログラムを複数のプログラム (以下，部分プログラムという) 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，“処理の委託に対する信頼性確保の問題” に対する解決策である．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．処理の多重化において，同一の処理を行う処理ノードの集まりを “ブロック”，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多数決をとるため，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ある．この，処理の多重化により処理時間が増加するという問題を解決するため，先行処理という手法が提案されている．

先行処理では，処理の多重化において，一番最初に得られた結果を暫定の結果として，投票待ちをせず，次の処理を開始する．そして，次の処理を実行している際に，前の処理結果が集まると，多数決を行い結果を確定させる．確定した結果と暫定の結果が一致していれば，そのまま処理を継続するが，異なっていた場合，先行して行った後続の処理をすべて取り消し，確定した結果で処理をやり直す．この，やり直しのことを “ロールバック” といい，ロールバックが頻繁に発生すると，先行処理の効果が失われてしまう．先行処理において，ロールバックの発生回数を低減させるための手法として，閾値暫定法がある．閾値暫定法とは，一番最初に得られた結果で処理を先行するのではなく，ある一定数の同一の結果が得られた時点で処理を先行するという手法である．ここでの，ある一定数のことを暫定閾値という．

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，閾値暫定法を取り入れたエクスターナルグリッドである．本稿では，同ブロック内に存在する悪人は，必ず間違った結果を返し，また，必ず共謀することとする．また，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 $k = 5$，尺度母数 $\theta = 2/5$，期待値 2 に基づいたガンマ分布に基づくものとし，分布を図 1 に示す．

4.1 信頼性

信頼性は，各部分プログラムにおいて，投票後の確定した結果が，部分プログラムごとに全て正しいかどうかで評価を行う．部分プログラムごとに確定した結果が全て正しければ，そのグリッドのプログラムの最終的な処理結果は正しい結果となる．しかし，部分プログラムのうち，一つでも間違った結果を確定した結果とし，処理を進めた場合，プログラムの最終的な処理結果は誤ったものとなってしまう．

Consideration of trade-off relationship among reliability, confidentiality and processing power in an external grid using advanced processing
Y. Tanaka, Department of Computer Science, Faculty of Engineering, Ehime University
K. Endo, Y. Higami, S. Kobayashi, Graduate School of Science and Engineering, Ehime University

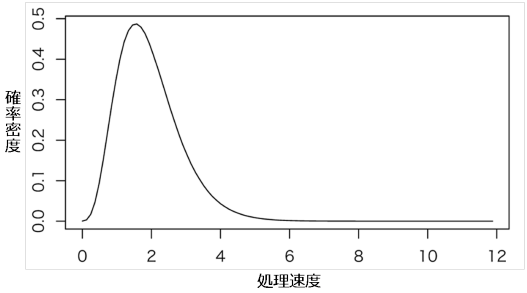

図 1　計算機の性能分布

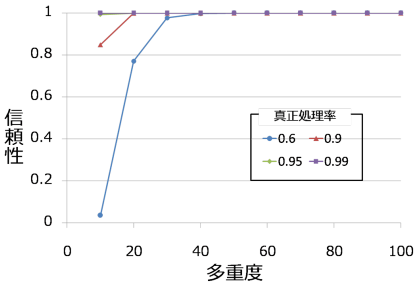

図 2　多重度と信頼性の関係

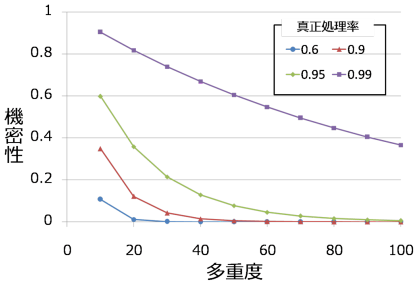

図 3　多重度と機密性の関係

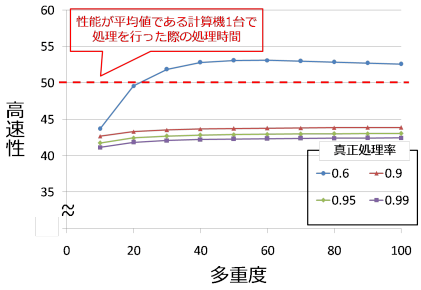

図 4　多重度と高速性の関係

ある一つの部分プログラムが正しくなる確率 P は

$$P = \sum_{n=0}^{m-V_k} {}_mC_m p^{m-n}(1-p)^n$$

となる．ここでの p は真正処理率，m は多重度，V_k は確定閾値である．ここで，真正処理率とは，一つのノードが正しい結果を返してくる確率のことである．そして，この P を用いて，部分プログラム全てが正しくなる確率 P_r は

$$P_r = P^D$$

と示すことができ，これを信頼性の評価値とする．

4.2　機密性

プログラムの一部，または，すべてが悪人に取得された場合，その部分は漏洩したものと表現し，取得されなかった部分は保護できたと表現する．機密性は，全体のうち，保護できたプログラムの割合を用いて評価を行う．

一つの部分プログラムを保護することができる確率 R は多重度 m と真正処理率 p を用いて，

$$R = p^m$$

と表すことができる．機密性の期待値 P_c を以下の式で示し，これを機密性の評価値とする．

$$P_c = \sum_{k=0}^{D} {}_DC_k(1-R)^{D-k}R^k\frac{k}{D}$$

ここで，D はプログラム分割数である．

4.3　高速性

高速性は，グリッドにおいて，処理が完了するまでの時間によって評価を行う．また，高速性についてはシミュレーションによって評価を行った．暫定閾値の値は多重度に対して 3 割の値とする．

5　結果と考察

それぞれの指標について，定量的に示した結果を図 2, 図 3, 図 4 に示す．また，すべての指標について，分割数 100 とした．結果より，多重度を増加させるにつれて，信頼性は向上するが，高速性・機密性は低下してしまうことがわかる．図 2 より，多重度を 30 まで上げると，図 2 中のすべての真正処理率について，9 割以上の信頼性を確保することができるということがわかる．しかし，図 3 より，8 割以上の機密性を確保するには多重度をは 20 以下でなければならないことがわかる．本稿では，多重度の値を 10 から 10 刻みとしたが，機密性では多重度 1 から 20 の範囲において変化の割合が大きいため，さらに詳細な実験を行う必要がある．図 4 より，高速性に関しては，先行処理によって，性能が平均値である計算機 1 台で処理を行った場合と比べて，真正処理率が 0.9 以上である場合は処理時間を短縮することができた．

6　まとめ

本稿では，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・信頼性について定量的に評価を行い，トレードオフの関係性を示した．今後は，閾値暫定法以外の手法でのトレードオフ関係についても示す必要がある．

謝辞

本研究は JSPS 科研費 JP26330105 の助成を受けたものです．

参考文献

[1] 合田卓矢 樋上喜信 小林真也 (2009) “エクスターナルグリッドを対象とした処理目的の隠蔽法” マルチメディア通信と分散処理ワークショップ 2007 論文集 2007(9), pp.91-92