6S-07

エクスターナルグリッドの処理結果を誤りに導くことを意図する悪人がもたらす影響の定量的評価

山口 晃右† 遠藤 慶一† 樋上 喜信† 小林 真也†
†愛媛大学大学院理工学研究科

1 はじめに

エクスターナルグリッドは，グリッドコンピューティングに分類される分散処理技術の一つである．エクスターナルグリッドは，インターネットに接続された計算機で構成されている．従って，実質的に無制限に計算資源を獲得でき，安価に HPC を実現できる．しかし，営利目的でのグリッドサービスの成功例は無い．インターネットに接続された不特定多数の計算機の管理者の中に不正行為を働く “悪人” が存在するため，エクスターナルグリッドの安全性が十分に保証されないためである．本稿の目的は，エクスターナルグリッド (以降、単にグリッドと呼ぶ．) の安全性の向上を図り，安全性の裏付けを行うことである．特に，グリッドに依頼されたジョブの処理結果を誤りに導くことを意図する悪人がもたらす影響に注目する．上記のような悪人が存在するグリッドの，機密性，高速性，信頼性の関係性を示し，定量的な評価を行う．

2 セキュアプロセッシング

グリッド上で計算する計算機を，“ノード” と呼ぶ．また，悪人が所有するノードを “悪人ノード” と呼ぶ．セキュアプロセッシング [1] は，悪人による不正行為のリスクを軽減する技術の集合である．不正行為には，グリッドに依頼されるジョブの内容に対する “不正解析” と，ジョブの実行結果に対する “改竄” がある．以下に，セキュアプロセッシングの一部を示す．

プログラム分割 グリッドに依頼されたジョブを分割し，プログラム断片を生成する．各断片は，各ノードに実行される．不正解析に効果がある．

処理の多重化 改竄対策の一つである．同種のプログラム断片を “多重度” 台のノードで実行する．その同種の断片の処理を行うノードの集合を “ブロック” と呼ぶ．ブロック内の各ノードの実行結果で投票を行うことで，処理結果の信頼性を高める．

3 網羅法

処理の多重化では, ブロック内のノード間で，処理完了時間に差が現れる．ブロック内で最速のノードの処理結果を用い，先行して処理を進めることで，グリッド全体の高速化を行える．これを先行処理という．ただし，先行処理をするノードの結果が，正しくない場合がある．この場合，先行していた処理は無効となり再処理が発生する．そこで，ブロック内の各ノードの出す結果毎に，網羅的に先行処理を行うことで再処理を無くし，より高速化ができる．これを “網羅法” という．網羅法は安定して高速化できる反面，利用するノード数が増加する欠点がある [2].

Quantitative evaluation of influence by malicious owners intending to alter processing results in an external grid
†Kosuke Yamaguchi †Keiichi Endo †Yoshinobu Higami †Shinya Kobayashi
†Graduate School of Science and Engineering, Ehime University

4 悪人集団の目論見と対策

グリッド上の悪人は，集団を形成する場合がある．集団を形成した場合，各悪人が単独である場合よりもリスクが出る．

本稿では，グリッドに依頼されたジョブの処理結果を，誤りへと導くことを目論む悪人集団について議論する．具体的には，同一ブロック内の全悪人ノードは、同一の誤った実行結果を返す．この様な悪人集団による影響には，以下のものが考えられる．

- 各悪人ノードが取得した断片を持ち寄ることによる不正解析のリスクの増加 [3]
- 依頼されるジョブの実行結果の信頼性の低下

二つ目の影響は，多重度を大きくすることで小さくできると考えられる．しかし，多重度の増加は，グリッドを構成する悪人ノードの台数の増加に繋がる．この現象は，悪人集団による不正解析のリスクを増加させるので，機密性を低下させる恐れがある．

高速性も，多重度の増加や悪人ノードの増加によって，影響があると考えられる．

そこで，前述した目論見を持った悪人集団が潜伏したグリッドの信頼性，機密性，高速性の三つの指標を評価をする．更に，グリッドの利用者が安全に利用できるようなグリッドの状態を定量的に示す．

5 評価方法

信頼性を，グリッドに依頼されたジョブが返す実行結果の正しさに注目し評価する．最終的な実行結果が正しさは，依頼されたジョブの実行結果が，悪人ノードが返す結果を元に導き出されるか否かで決める．

機密性を，悪人集団が取得する最大連続長に注目して評価する．悪人集団が不正解析を行う場合，集団全体が取得する連続長が長い方が，不正解析の難易度が下がると考えられる．悪人集団が取得する最大連続長を求めることで，悪人集団に盗視されるリスクを定量的に求められる．

高速性を，グリッドに依頼されたジョブが完了するまでの時間でもって評価する．より時間が短ければ，グリッドの性能が高いことを示している．

以上の三つの指標を求める際，連続したプログラム断片数，多重度，悪人の存在確率を入力とするシミュレーションを行う．以下に条件を示す．

- グリッドを構成するノードは，無数に存在する．
- ノードに含まれる悪人を識別できず，悪人ノードは存在確率に応じてグリッド中に存在する．
- グリッド上の悪人は 1 つのグループに属しており，4 節で述べた振る舞いをとる．
- 各ノードの処理性能は，各ノードが単位時間当たりに処理できるプログラムのサイズであるとし，形状尺度 $k = 5$，尺度分母 $\Theta = 2/5$，期待値 2 となるガンマ分布に従う．

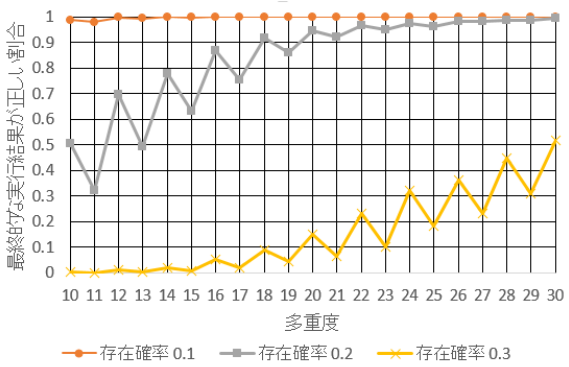

図 1: 多重度と信頼性の関係

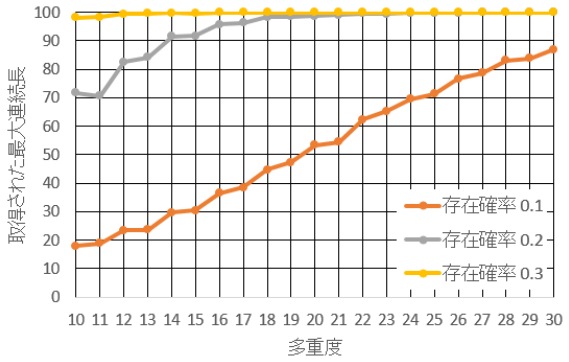

図 2: 多重度と機密性の関係

- 連続したプログラム断片数は 100 である．
- 入力された同一条件での試行を 1000 回行う．

6 評価結果と考察

6.1 信頼性

多重度の変化と信頼性の関係を示した図が，図 1 である．横軸は多重度を表す．縦軸は，1000 回の試行のうち，正しい実行結果を返した割合である．図中では，悪人の存在確率が異なる場合のグラフが並べられている．図 1 より，悪人の存在確率が 0.1 の場合，多重度 10 以上なら高い信頼性を維持していることが分かる．存在確率が 0.2 であれば，正答率 90%を確保するには多重度が最低 20 必要であるといえる．

以上より，多重度の増加が信頼性の向上に繋がることが分かる．

6.2 機密性

多重度の変化と機密性の関係を示した図が，図 2 である．横軸は多重度を表す．縦軸は，悪人集団に取得された連続するプログラム断片の最大連続長の平均である．前節と同様に，存在確率が異なる場合のグラフを比較している．図 2 では，存在確率が 0.2 の場合，多重度が 20 で盗視された最大連続長は約 98 である．多重度 20 は，図 1 より，正答率を 90%以上に維持するための多重度であった．つまり、高い信頼性を維持するためには，機密性の低下が発生するといえる。

以上より，多重度の増加が，悪人集団に取得される最大連続長を増大させ，機密性の低下を発生させるといえる．

6.3 高速性

グリッドに依頼されたジョブが完了するまでの処理時間と多重度の関係を表したものが，図 3 である．横軸は多重度を表す．縦軸は，グリッドが最終的な実行結果を返すまでにかかる時間の平均を表している．図 3 より，多重度の増加により，処理時間が減少する傾向にあることが見て取れる．例えば，存在確率が 0.2 の場合，多重度 10 における処理時間と多重度 30 における処理時間では，約 3 割程の短縮がなされている．

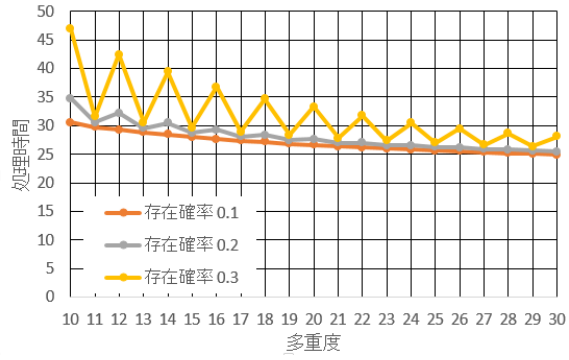

図 3: 多重度と高速性の関係

以上より，多重度が大きい方が，より高性能なノードが参加する投機的な効果を得やすいため，グリッド全体の処理が高速化されるといえる．

7 まとめ

本稿では，グリッドに依頼されたジョブの実行結果を誤りに導こうとする悪人集団が，グリッドに与える影響について定量的に評価した．また，信頼性，機密性，高速性の三性能の関係を示し，利用者が安全に利用できる状況を定量的に示した．

多重度の増加が信頼性の向上と共に，高速性に好影響を与えることが示せた．一方で，信頼性を確保するための多重度の増加は，機密性を著しく低下させる．ただし，先行研究で提案された保護処理 [4] を利用することで，機密性の低下を抑えられる．多重度を大きくし，信頼性と高速性を高い水準で維持する場合，保護処理と合わせて利用する必要があると考えられる．

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] 木下 裕司，小林 真也 : “エクスターナルグリッドを対象としたセキュアプロセッシングにおける安全性の研究”，愛媛大学大学院理工学研究科博士前期課程情報工学専攻，修士論文，(提出日)2007/1/31.

[2] 広瀬 吉隆，稲元 勉，樋上 喜信，小林 真也 : “セキュアプロセッシングにおける先行処理による処理時間改善に対する定量的評価”，第 14 回情報科学技術フォーラム (FIT2015) 講演論文集，Vol.4,pp.241-242，2015.

[3] 山口 晃右，稲元 勉，樋上 喜信，小林 真也 : “エクスターナルグリッドに対する依存関係を利用した不正解析のリスクを軽減する手法”，情報処理学会第 78 回全国大会論文集，5660，2016.

[4] Kosuke Yamaguchi, Tsutomu Inamoto, Keiichi Endo, Yoshinobu Higami, and Shinya Kobayashi,“Evaluation of Influence Exerted by a Malicious Group’s Various Aims in the External Grid”, Hard and Soft Computing for Artificial Intelligence, Multimedia and Security, vol 534, pp.112-122, 2016.