6L-02

グリッドコンピューティングにおける悪意を持つノードの共謀関係が信頼性に与える影響の定量的評価

松重　直起†　　藤橋　卓也‡　　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コンピュータ資源を用いて，高い処理性能や記憶容量を仮想的に得る技術である．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コンピュータを利用対象としてグリッドを構成することで，高性能な処理能力，計算容量を得られる．一方，利用者の中に悪意を持った第三者が混入する危険性がある．悪人が保持するコンピュータリソースを利用した場合，実行プログラムの内容解析や実行結果の改竄をされてしまう恐れがある．これらの問題の解決策の一つとして，セキュアプロセッシングが挙げられており，その中でもプログラム分割や処理の多重化が提案されている．グリッド上で処理を依頼するコンピュータを管理ノード，処理を行うコンピュータを処理ノード，プログラムの解析・改竄といった不正行為を行う処理ノードを悪人と呼ぶ．処理の多重化では，同一の処理を複数の処理ノードに依頼し，返ってきた結果に多数決を行い処理結果を決定する．これにより，誤った処理結果を採用しづらく，処理結果が改竄されたものでないと信頼できる．しかし，処理ノードに選ばれた悪人同士が示しを合わせ同一の誤った処理結果を行うと，多数決の結果誤った処理結果が採用される恐れがある．悪人同士が共謀を行うには，悪人同士の交友関係を持っている必要がある．

本研究では，悪人が共謀した際の処理の多重化の信頼性を，悪人の共謀関係の想定としてスモールワールド性の特徴とスケールフリー性の特徴の両方の特徴を持ったネットワーク上での管理ノードが正しい処理結果を採用する確率を調査することで評価し，多重化の有効性について考察することを目的とする．

2　セキュアプロセッシング

セキュアプロセッシングとは，グリッド上の悪人が行う不正な解析結果・改竄へのために考案された技術の総称である．

2.1　プログラム分割

プログラム分割は，依頼するプログラムを複数のプログラム断片に分割し，処理を依頼する．プログラム断片に分割することにより，一つの処理ノードに渡る情報量が減少するため，不正な解析に対して効果がある．

Quantitative evaluation of influence of collusion of malicious nodes in grid computing on reliability
†N. Matsushige
Department of Computer Science, Faculty of Engineering, Ehime University
‡T. Fujihashi , K. Endo . S. Kobayashi
Graduate School of Science and Engineering, Ehime University

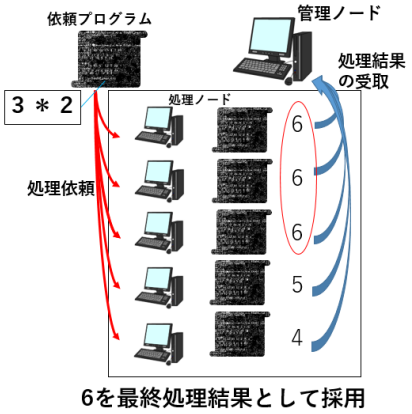

図 1: 正しい処理結果が採用される場合

2.2　処理の多重化

同一の処理を依頼する複数の処理ノードを処理ノード群，処理ノードの数を多重度と呼ぶ．

処理の多重化は，処理を一つの処理ノードだけに依頼するのではなく，複数の処理ノードに依頼し，最終的な処理結果を多数決で確定する．処理ノード群中に不正な結果を返してくる処理ノードが存在していても，他の正しい結果を返すノードによって，多数決後の処理結果は正しい結果となる．これにより，不正な処理結果を最終処理結果として採用する恐れを減らすことができるため，処理結果の信頼性を確保することが出来る．図 1 に処理の多重化の例を示す．

3　処理の多重化における悪人の共謀

処理の多重化において，処理ノード群に複数の悪人が存在するとき，悪人同士が共謀して不正な同一の処理結果を返す恐れがある．図 2 に悪人の共謀による処理の多重化への影響を示す．悪人同士の共謀によって，誤った処理結果が多数派となった場合，誤った処理結果が最終処理結果として採用されてしまう．すなわち，処理の多重化の改竄対策効果が有効に機能しない恐れがある．現在，悪人の共謀が処理の多重化にもたらす影響が定量的に評価されておらず，悪人の共謀を想定した処理の多重化の改竄対策効果が有効か検証する必要がある．

悪人集団の処理ノードが同一の誤った処理結果を返すには，お互いに意思疎通を行うグループを構成する必要がある．そのようなグループの大きさが，多重化の有効性に対して強い影響を及ぼすと考えられる．つまり，処理ノード群内の悪人集団の悪人同士がどのような繋がりを持っているかということが重要となる．

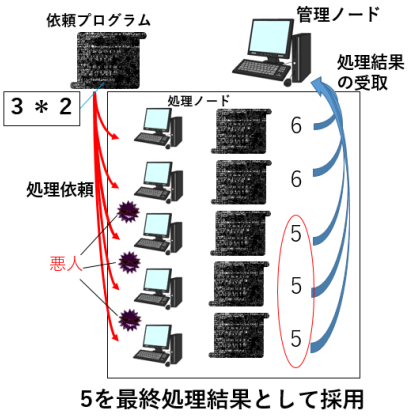

図 2: 誤った処理結果が採用される場合

4 悪人間の共謀関係

悪人同士で共謀するには，悪人同士が繋がりとして，現実の悪人同士が知り合いであり意思疎通を行っていると考えられる．よって，悪人の繋がりは現実の交友関係をグラフ化したネットワークと捉えられる．交友関係をグラフ化したネットワークは，主に以下の 2 つの特徴を持っている．[1]

- スモールワールド性

  極一部のノードが大多数のエッジを持ち，残りの殆どのノードは少数のエッジしか持たない

- スケールフリー性

  頂点の次数の分布がベキ則になる．また，任意の 2 つのノード間の距離が一定範囲内に収まる

5 提案

悪人の共謀関係を表すのネットワークとして，スモールワールド性及びスケールフリー性の両方の特徴を兼ね備えた階層ネットワークを構成する．構成した階層ネットワーク上の悪人を想定しで，悪人が含まれたネットワーク上で処理の多重化のシミュレーションを行う．

6 階層ネットワーク

階層ネットワークは，Ravasz と Baarasi によって 2003 年に提唱されたネットワークモデルである．この階層モデルは，図 3 のアルゴリズム [1] に従って生成される．

このアルゴリズムによって生成された階層モデルは，スモールワールド性の特徴である，クラスター係数 C (0≦C≦1) が C ≈0．743 と大きい値を取る．また，スケールフリー性の特徴である頂点の次数分布がベキ則に従う．このことから，現実の交友関係を表したネットワークとして，階層ネットワークが適しているため，本研究では階層ネットワーク上で多重化の処理の依頼を行った．

7 評価

処理の多重化のシミュレーションを行うにあたり，悪人の共謀関係は，悪人と直接繋がりを持つを悪人を同じ誤った処理結果を返す悪人グループとし，悪人グループが異なると異なる誤った処理結果を返すとする．また，評価を行う多重化の信頼性を，依頼する処理 1 回における正しい処理結果が返ってくる確率とし，選定されるノードに左右されにくくするために複数回試行して正しい処理結果が返ってきた回数を試行回数で除算したものとする．

階層モデル

1. N_0点からなる完全グラフを作る.中心の頂点vを1つ決める.
2. この完全グラフのコピーをN_0-1個追加し，vのコピー以外の新しい頂点それぞれと,元のvを繋ぐ.頂点数はN_0^2となる
3. 新しい枝を作らなかった頂点は,中心の仲間入りをする.
4. t=1でできたネットワークのコピーをN_0-1個追加する.中心の属する頂点以外の点から,大元の中心vに枝をはる.
5. ステップ3と4を時刻Tまで繰り返す.

図 3: 階層モデルのアルゴリズム

依頼する処理 1 回における正しい処理結果が返ってくる確率 P は，正しい処理結果が採用された回数 L，処理の依頼の総試行回数 m を用いて $P = L/m$ と表せる．作成したネットワーク上で，最初に悪人となるノードをランダムに選定したのち，不正な処理結果を返す悪人の共謀関係を作成する．そののち，処理ノードを多重度の数だけランダムに選定し，多重化のシミュレーションを 1000 回行った．総ノード数 125 のシミュレーション結果を表 1 に示す．正しい処理結果が採用される確率は，総ノード数に対する悪人の割合が大きくなると同グループの悪人が選定されやすく共謀を行いやすいため小さくなる．また，多重度が大きくなるほど同グループの悪人が選定されづらく共謀が行いにくいため正しい処理結果が採用される確率は大きくなる．

表 1: 正しい処理結果の採用確率

		総ノード数に対する悪人の割合				
		1 割	2 割	3 割	4 割	5 割
多重度	3	99.8%	98.2%	93.8%	83.4%	70.1%
	5	100%	99.4%	95.5%	87.2%	71.3%
	7	100%	99.6%	97.4%	89.4%	70.4%
	10	100%	100%	99.3%	93.8%	79.4%
	20	100%	100%	99.7%	95.5%	77.5%

8 終わりに

階層ネットワーク上での悪人が共謀した場合の処理の多重化の信頼性は，悪人の存在割合が大きい場合に無くなってしまう．今後の予定として，悪人の共謀がない場合の信頼性や，その他のネットワーク上での処理の多重化の信頼性と比較を行う必要がある．

参考文献

[1] 矢久保孝介 (2013)”複雑ネットワークとその構造”共立出版

[2] 増田直紀・今野紀雄 (2010-2013)”複雑ネットワーク: 基礎から応用まで”近代科学社