5V-06

悪人の共謀がグリッドコンピューティングの機密性・信頼性に与える影響の定量的評価

松田 匠真† 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機を利用し, 高性能な処理能力や記憶容量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コンピュータを利用してグリッドを構成する. もし, このグリッドに悪意を持つ人間（以下悪人）が所有するコンピュータが混入した場合, 処理内容が不正に取得される「処理内容の解析」や, 処理による結果が正しいものではない「処理結果の改竄」といった不正行為を行う可能性がある. 悪人が不正行為を行う際, 悪人同士が共謀すると, 不正行為を行いやすい状況になる.

不正行為の対策としてセキュアプロセッシングが挙げられる. このセキュアプロセッシングには, プログラム分割や処理の多重化が提案されている.

先行研究 [1] では, 処理の多重化の信頼性の評価をする際に, 悪人の共謀関係をネットワークと考え, スモールワールド性を持つネットワーク, スケールフリー性を持つネットワーク, またスモールワールド性とスケールフリー性の両方を持つネットワークに対して, 処理の多重化を検証している.

本研究では, スモールワールド性とスケールフリー性を持つネットワークにおいて, 悪人の共謀における解析・改竄のリスクの定量的評価を行う. その上でグリッド管理者が処理依頼を行う際に, 処理目的に応じて, どのようなパラメータの設定をすればリスクを回避できるのかを示す.

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, グリッド上における不正行為の対策技術の総称である.

2.1. プログラム分割

プログラム分割は, 処理内容の解析への対策である. 処理を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）に分割し, 各プログラム断片を, 異なる計算機に処理依頼する. こうすることにより, 一つの処理ノードが取得するプログラムの量を減らすことになる. こうすることで, 処理ノードが悪人だった場合の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. 処理を依頼する際, 処理ノードを一つに限定するのではなく, 複数の処理ノードに依頼し, 複数の処理結果から多数決によって処理結果を決める. こうすることにより, 悪人のノードが不正な処理結果を返した場合でも, 複数の処理ノードを利用したことにより, 正しい処理結果が返ってくる. なお, 選択する処理ノードの数は多重度と呼ぶ.

3. 処理依頼時の悪人の共謀による影響

悪人の共謀が存在すると, 処理を依頼する側の人間が解析・改竄の不正行為にあう可能性が高くなる.

悪人の共謀が存在する際, プログラム分割を行った場合, 悪人ノード同士が取得した各プログラム断片を共有することにより, 悪人が多数のプログラム断片を取得することが可能になってしまう.

また処理の多重化では, 複数の処理ノードの中で, 同じ誤った処理結果を返す悪人ノードが過半数以上の場合, その処理結果は改竄されたものとなってしまう. これにより, 最終的な処理結果が正しくないものになってしまう.

よって, 悪人の人数が多くなると, 処理の多重化により選定される処理ノード中に, 悪人ノードが選ばれる可能性が高くなり, 悪人にプログラム断片を取得されてしまう可能性が高くなる.

このように, 悪人の共謀がある場合, 解析・改竄の両方のリスクに影響を与えてしまう恐れがある.

4. ソーシャルグラフ

ソーシャルグラフとは, 現実的な交友関係における, 各個人同士のつながりをモデル化したものである. 多くのソーシャルグラフには, スモールワールド性やスケールフリー性が存在する場合がある.

スモールワールド性は, 大規模なグラフであっても, 任意の 2 つのノードの距離が一定の範囲内に収まる性質である.

スケールフリー性は, グラフ中のごく一部のノードが大多数のエッジを持ち, 残り殆どのノードは少数のエッジしか持たない性質である.

本研究では, ソーシャルグラフにならって, 階層ネットワークを作成する. 階層ネットワークは以下の手順 [1][2] にて生成される.

step1 n 個の頂点からなる完全グラフ K_n を作成する. 中心の頂点 v を一つ決める.

step2 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のそれぞれと, 元の v を繋ぐ. 頂点数は N_0^2 となる.

step3 新しい枝を作らなかった頂点は, 中心の仲間入りをする.

Quantitative evaluation of the influence of collusion of malicious people on the confidentiality and reliability of grid computing
†T.Matsuda
Department of Computer Science, Faculty of Engineering, Ehime University
‡K.Endo, S.Kobayashi
Graduate School of Science and Engineering, Ehime University

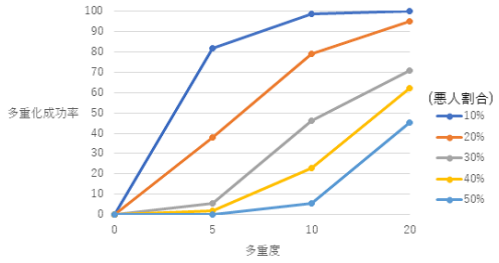

図 1: 多重化成功率 (総ノード数 64)

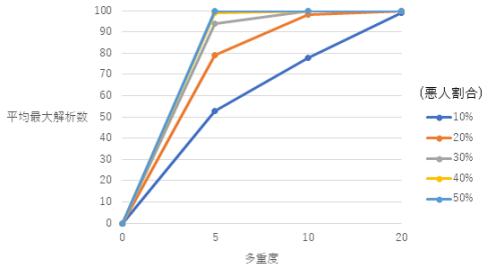

図 2: 平均最大解析数 (総ノード数 64)

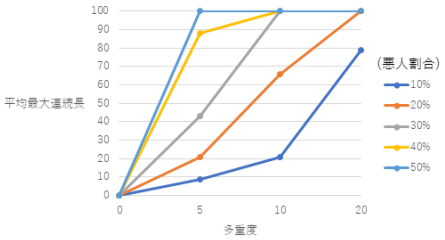

図 3: 平均最大連続長 (総ノード数 64)

step4 step1 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.

step5 step3 と step4 を繰り返す.

これにより生成されたネットワークは, クラスタ係数 $C(0 \leq C \leq 1)$ が $C \approx 0.743$ と大きな値をとることから, スモールワールド性を持つネットワークであるといえる. また, 頂点の次数分布がベキ則に従うことから, スケールフリー性を持つネットワークであるといえる. よってこの階層ネットワークはスモールワールド性とスケールフリー性をもつネットワークであるため, 本研究ではこの階層ネットワークを元に改竄・解析のリスクを評価する.

5. 処理の多重化のシミュレーション

作成した階層ネットワークを用いて, 処理の多重化のシミュレーションを行う.

作成した階層ネットワークにおいて,1 回の試行回数毎に悪人となるノードをランダムに選定し, 不正な処理結果を返す悪人の共謀関係を作成する. そして, プログラム分割数毎に処理ノードを多重度の数に従ってランダムに選定する. このシミュレーションを 1000 回行う.

6. 改竄・解析リスクの評価手法

改竄・解析の両リスクに関しての評価手法を示す.

改竄リスクは, グリッド管理者が処理依頼を行う際の, 最終的な処理結果が改竄されている確率とする. 試行回数 1000 回においてプログラム分割数中の 1 回でも処理の多重化を失敗した場合を,1 回の誤った処理結果とし, この回数を試行回数で除算したものとする. 各パラメータでどのような値の変化が見られるのかを元に考察する.

解析リスクは, 試行回数 1000 回における各試行回数の悪人グループが取得したプログラム断片の最大解析数と最大連続長の平均を求める. これらのシミュレーションでの数値の結果から, パラメータ毎にどのような値の変化が見られるのかを元に考察する.

7. 結果と考察

総ノード数 64 個とプログラム分割数 100 個に対して, 多重度 5・10・20, 悪人割合 10%から 50%で変化させた際の多重化成功率・平均最大解析数・平均最大連続長を図 1,2,3 に示す. 図 1 では, 多重度が大きくなると処理の多重化が成功する割合が高くなっている. このことから, 改竄リスクの低減に多重化が有効であることがわかる. さらに図 2,3 では, 多重度を大きくすることにより, 悪人が取得するプログラムの数とその連続長が多くなることがわかる. このことから, 解析のリスクは多重度を大きくすると増大することがわかる. 上記より, 多重度における解析・改竄リスクはトレードオフ関係にあるといえる. よって, 処理依頼する際の目的が, 処理内容の解析を防ぐことに重点を置いている場合, 多重度は小さい値の方が良いと言える. また, 処理内容の改竄を防ぐことに重点を置いている場合, 多重度は大きい方が良いといえる.

8. 終わりに

本稿では, スモールワールド性とスケールフリー性をもつ階層ネットワーク上での多重化処理における, 改竄・解析リスクについて, 定量的に評価を行った. その結果処理の多重化における多重度は, 両リスクにおいてトレードオフの関係にあることを示した. 今後の課題としては, 他のネットワーク上での各リスクの比較や, 悪人の割合・多重度をさらに細分化した際の各リスクの比較を行う必要がある.

参考文献

[1] 松重直樹, 藤橋卓也, 遠藤慶一, 小林真也 (2019)“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” 情報処理学会第 81 回全国大会論文集

[2] 矢久保孝介 (2013)“複雑ネットワークとその構造” 共立出版