7X-04

リスト管理手法と保護処理を用いたエクスターナルグリッドにおける機密性・高速性の定量的評価

三浦 崇考徹 † 遠藤 慶一 ‡ 小林 真也 ‡
愛媛大学工学部工学科 † 愛媛大学大学院理工学研究科 ‡

1 はじめに

ネットワーク上の計算機を利用して分散処理を行うことで，高い処理能力や記憶容量を得ることができるグリッドコンピューティングと呼ばれる技術がある．グリッドコンピューティングはインターナルグリッドとエクスターナルグリッドの二つ分類される．インターナルグリッドはイントラネット上の計算機を利用するため，利用できる計算機の数に限りはあるが安全性は高い．それに対して，エクスターナルグリッドはインターネット上の計算機を利用するため，無数の計算機を利用できるので処理性能は高くなるが，悪意を持った人間の計算機（悪人）が紛れ込み，不正行為を行う可能性がある．

2 研究背景

2.1 悪人による不正行為

悪人が行う不正行為には，不正な解析と処理結果の改竄が考えられる．不正な解析は，処理を依頼された悪人が依頼されたプログラム内容を解析し，プログラム内容やデータを盗むことである．処理結果の改竄とは，処理を依頼された悪人が意図的に誤った結果を返すことである．

2.2 セキュアプロセッシング

不正な解析への対策として，プログラム分割，保護処理，処理結果の改竄への対策として，処理の多重化がある．

2.2.1 プログラム分割

処理を依頼するプログラムを複数の断片に分割し，異なる計算機へ処理を依頼することをプログラム分割という．プログラムを複数の断片に分割することで 1 つのプログラム断片が持つ情報量を抑えることができる．

2.2.2 保護処理

信頼できる処理ノードに依頼して処理することを保護処理と呼び，保護処理されるプログラム断片のことを被保護断片という．連続したプログラム断片を等分する位置に保護処理を施すことで，プログラム断片の連続長を最小化できる．そのため，悪人が取得できる連続長を制限することができる．

2.2.3 処理の多重化

処理の多重化とは，一つの処理を複数の処理ノードに依頼し，返された結果に対して多数決処理を行い，処理結果を決める手法である．多数決処理を行うことで処理結果が正しくなる可能性を上げることができる一方で，同一の処理結果の数が確定閾値を満たすまで次の処理に移ることができないため，処理時間が増加するといった問題点がある．

2.2.4 先行処理手法

処理の多重化の問題点である処理時間の増加を改善する手法として先行処理がある．先行処理とは，多数決処理の際に確定閾値と同数以上の処理結果が揃う前に，早く結果を返した処理ノードの処理結果を暫定的な結果として扱い，処理を進める手法である．多数決処理の結果が暫定的な結果と一致しなければ，ロールバックと呼ばれるやり直し処理を行う．

2.2.5 リスト管理手法

先行処理の問題点であったロールバックによる処理時間の増加に対する対策としてリスト管理手法がある [1]．リスト管理手法とは，“真正な処理結果のみを返す”，“処理時間が閾値よりも高速である”の 2 点を満たす処理ノードをリスト管理し，そのリストから処理ノードを選ぶ手法である．しかし，リスト内に多数の解析を行う悪人が存在した場合，機密性が低下する危険性がある．

2.3 研究目的・目標

リスト管理手法と保護処理を組み合わせることで悪人集団に取得されるプログラム断片の連続長を制限することができると考えられる．しかし，保護処理を用いることで，被保護断片を処理する処理ノードは信頼できる処理ノード 1 台のみとなり，先行処理による高速性向上の効果を受けられないため，高速性に悪影響を及ぼす可能性がある．そこで，本研究の目的，目標を以下のように定める．

リスト管理手法と保護処理を用いたエクスターナルグリッドにおいて，機密性，高速性の観点から両手法を組み合わせることの有効性を示し，エクス ターナルグリッドの安全性を高める．また，リスト管理手法と保護処理を用いたエクスターナルグリッドにおいて機密性・高速性を定量的に評価し，保護処理を用いない場合との比較，考察を行う．

3 評価手法

本研究では，機密性は評価式，高速性はシミュレーションによって求める．また，機密性，高速性を求める際は，多重度

Quantitative Evaluation of Confidentiality and Processing Time in External Grids Using List-based Node Management Method and Protective Treatment

† T. Miura
Department of Engineering, Faculty of Engineering, Ehime University
‡ K. Endo, S. Kobayashi
Graduate School of Science and Engineering, Ehime University

m が 5，インターネット上の悪人の存在確率 V_i が 10%，ホワイトリスト内の改竄を行う悪人の存在確率 V_{wt} が 10%，ホワイトリスト内の解析を行う悪人の存在確率 V_{wa} が 50% を条件とする．また，機密性を求める際のプログラム分割数 D は 100 とする．

3.1 機密性評価における条件

インターネット上に存在する悪人とホワイトリスト内に存在する悪人は 1 つの集団に属するものとする．悪人が 1 つの集団に属することで悪人同士が不正な解析による処理内容やデータを共有できる．そのため，悪人集団に処理データやデータの依存関係を把握され，機密性の低下につながる．

ホワイトリストから選択する処理ノード n は多重度 m の過半数未満で最大の整数とする．ホワイトリストから選択する処理ノード数を制限することで，ホワイトリスト内の処理ノードの枯渇を防ぐことができる．

3.2 機密性の評価手法

プログラム分割数 D 個のうち，悪人集団に取得されるプログラム断片の連続長が k 個になる確率を機密性の評価指標として用いる．この指標を用いるのは，悪人集団に取得されるプログラム断片の連続長が大きいほど，処理内容やデータの解析リスクが高まるためである．

3.2.1 機密性の評価式

プログラム分割数を D，被保護断片の数を q とすると，保護処理によって最小化されたプログラム断片の連続長は S_l または S_s となる．このとき，連続長が大きい方を S_l，小さい方を S_s とする．

$$S_l = \lceil \frac{D-q}{q+1} \rceil \tag{1}$$

$$S_s = \lfloor \frac{D-q}{q+1} \rfloor \tag{2}$$

また，S_l，S_s のそれぞれの個数 α，β は式 (3)，式 (4) で表される．

$$\alpha = D - S_s(q+1) - q \tag{3}$$

$$\beta = (q+1) - \alpha \tag{4}$$

多重度 m が奇数の場合，保護処理によって連続長が S_l，S_s に分割されたときの悪人集団が取得するプログラム断片の連続長が k になる確率を $PO_{pml}(k)$，$PO_{pms}(k)$ とすると，悪人集団が取得するプログラム断片の連続長が全体で k になる確率 $PO_{pm}(k)$ は式 (5) となる．

$$PO_{pm}(k) = 1 - \{(1 - PO_{pml}(k))^{\alpha}(1 - PO_{pms}(k))^{\beta}\} \tag{5}$$

多重度 m が偶数の場合，保護処理によって連続長が S_l，S_s に分割されたときの悪人集団が取得するプログラム断片の連続長が k になる確率を $PE_{pml}(k)$，$PE_{pms}(k)$ とすると，悪人集団が取得するプログラム断片の連続長が全体で k になる確率 $PE_{pm}(k)$ は式 (6) となる．

$$PE_{pm}(k) = 1 - \{(1 - PE_{pml}(k))^{\alpha}(1 - PE_{pms}(k))^{\beta}\} \tag{6}$$

3.3 高速性評価における条件

本研究では，処理ノードの処理性能の分布は，形状尺度 $k = 5$，尺度母数 $\theta = \frac{2}{5}$，期待値 2 に基づくガンマ分布に従った処理性能と定義する．

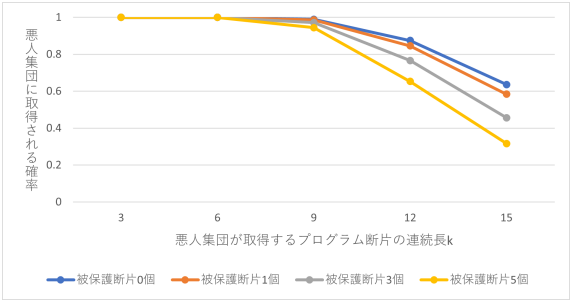

図 1　悪人集団が取得するプログラム断片の連続長 k を変化させたときの悪人集団に取得される確率の変化

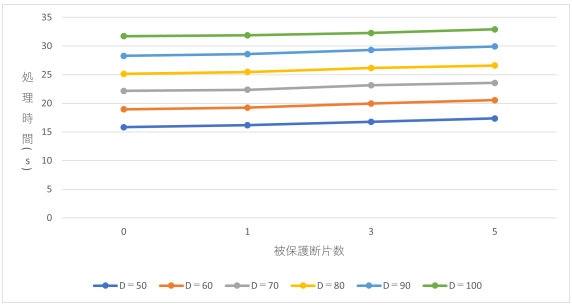

図 2　被保護断片数を変化させたときの処理時間の変化

3.4 高速性の評価手法

リスト管理手法保護処理を用いる場合，リスト管理手法のみの場合でそれぞれ 1000 回処理を繰り返し，得られた処理時間の平均値を最終的な処理時間とする．

4 結果・考察

4.1 機密性

悪人集団が取得するプログラム断片の連続長 k を変化させたときの悪人集団に取得される確率の変化を図 1 に示す．被保護断片 0 個は保護処理を用いていないことを示す．被保護断片の数が多くなるほど取得される確率は低くなっていることから，機密性の観点からみるとリスト管理手法と保護処理の組み合わせは有効であるといえる．

4.2 高速性

被保護断片数を変化させたときの処理時間の変化を図 2 に示す．被保護断片の数が増えても処理時間には大きな変化がないことがわかる．このことから，リスト管理手法と保護処理の組み合わせによる高速性への影響は小さいといえる．

5 おわりに

今後の課題として，本研究では先行処理手法に網羅法を採用したが，異なる先行処理手法での機密性，高速性の評価，考察が必要である．

参考文献

[1] 伊賀 俊輔，遠藤 慶一，小林 真也，“リスト管理手法を用いたエクスターナルグリッドにおける信頼性の定量的評価”，情報処理学会第 85 回全国大会講演論文集，2023.