6U-03

エクスターナルグリッドにおいて 処理ノードの処理性能が機密性に及ぼす影響の評価

大西 伊吹 † 遠藤 慶一 † 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，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し，分散処理を行う技術である．しかし，インターネット上の計算機は，処理結果の改竄や，処理内容の不正な取得を行う可能性がある．グリッドを構成し，実際に処理を行うインターネット上の計算機を処理ノードと呼び，そのうち処理内容の不正な取得を行うものを潜伏窃取者と呼ぶ．これらの問題を解決するためのセキュアプロセッシングや，それに伴う処理時間の増加を抑えるための先行処理が研究されているが，実用に足る機密性を得られていない．また，機密性と高速性はトレードオフの関係にあることが示されており，この 2 つの指標を両立することは難しい [1]．本稿では，処理ノードの処理性能が機密性に与える影響を示し，その結果を基に既存の方法と同等の高速性を維持しながら機密性を向上させる手法を提案する．

2. これまでの機密性と高速性向上のための取り組み

これまでの取り組みとして，プログラム分割や処理の多重化，先行処理等が研究されている．

2.1. プログラム分割

プログラム分割は，処理内容の不正な取得への対策である．処理ノードに依頼するプログラムを複数に分割し，それぞれを別の処理ノードへ依頼する．分割した個々のプログラムをプログラム断片と呼ぶ．各プログラム断片の処理を別の処理ノードへ依頼することで，潜伏窃取者が取得する情報量を抑えることができる．

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．1 つのプログラム断片の処理を複数の処理ノードへ依頼し，各処理ノードから得られた結果に対して多数決で処理結果を確定する．同じプログラム断片を処理する処理ノードの数を多重度という．本稿では，多数決を行うために必要な同一の処理結果の数を確定閾値と呼ぶ．確定閾値は多重度の過半数とし，多重度 N に対して $\lceil (N+1)/2 \rceil$ となる．

2.3. 先行処理

処理の多重化は，各処理ノードの処理性能にばらつきがあるため投票待ちが発生する．そのため，処理内容が確定するまでの時間が増加し，高速性が低下する．先行処理は，これを解消する方法である．

網羅法は，先行処理手法のひとつであり，処理ノードから新出の結果が返されるたびに新たな処理ノードで暫定的に処理を進める．多数決によって処理結果が確定した場合，その結果以外の先行処理は全て取り消す．この手法は，高速性の大きな向上が期待できる反面，利用する処理ノードの数が他の手法に比べて多いため，機密性が低くなりやすい．

3. 各指標の概念

3.1. 処理ノードの性能分布

本稿では，プログラム分割と処理の多重化，先行処理手法として網羅法を利用するエクスターナルグリッドを対象とする．また，シミュレーションでは，同一条件を 1000 回施行する．グリッドで利用する処理ノードの性能に関しては，以下の 2 パターンを取り扱う．

1. 処理ノードの処理性能を 0.1 から 5.1 の一様分布
2. 処理ノードの処理性能を形状尺度 $k = 5$，尺度母数 $\Theta = 2/5$，期待値 2 に基づくガンマ分布

3.2. 機密性

機密性は，プログラム断片が潜伏窃取者に取得される程度を表す指標である．本稿では，あるプログラム断片の処理結果が確定するまでに，その断片の処理を開始した処理ノードの数を用いて評価をおこなう．処理を開始した処理ノードの数が多いほど，不正に処理内容を取得されるリスクが高まり，機密性が低下する．

3.3. 高速性

高速性は，プログラム全体を処理するためにどの程度の時間が必要かという指標である．本稿では，3.1 の分布に従って決定された処理性能の逆数を断片 1 つの処理時間とし，その総和を用いて評価を行う．なお，処理ノードの選定やデータの送受信に必要な時間は，先行処理による改善が見込めず，環境による影響が大きいことから考慮しないこととする．

4. 処理ノードの処理性能が機密性に与える影響

本章では，処理ノードの処理性能のばらつきが機密性に与える影響を調査する．

4.1. 機密性への影響の評価方法

処理ノードの処理性能を以下の条件とし，各断片の処理ノードの利用数をシミュレーションする．なお，処理ノードの処理性能の分布に関しては，3.1 で示した一様分布を用いることとする．

- 利用する処理ノードの処理性能を 0.5 から 4.5 の範囲に制限
- 利用する処理ノードの処理性能を 1.5 から 3.5 の範囲に制限
- 制限なし

Evaluation of the impact of processing performance of processing nodes on confidentiality in the external grid
I. Oonishi, K. Endo, S. Kobayashi, Graduate School of Science and Engineering, Ehime University

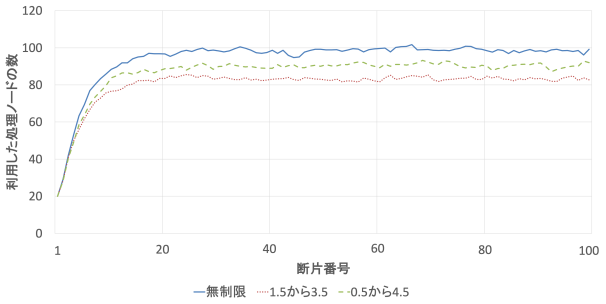

図 1: 断片番号ごとの利用した処理ノード数

表 1: シミュレーション条件

項目	条件
高性能閾値	2.0
低性能閾値	1.6
プログラム分割数	100
多重度	20
真正処理率	95%
処理ノードの処理性能分布	3.1 章に示すガンマ分布

また，各プログラム断片は全てに依存関係があるとし，親となる断片から順に断片番号 1,2,3…と呼ぶ．

4.2. 機密性への影響の評価結果

調査の結果，図 1 のような結果が得られた．ここから，処理ノードの処理性能を制限すると利用する処理ノードの数が少なくなるということがわかる．また，断片番号が大きくなると利用する処理ノードの数が大きくなっていき，徐々に収束している．これは，誤った先行処理に基づくさらなる先行処理の発生と，処理結果が確定した際に誤った先行処理を停止する網羅法の仕様のためと考えられる．これより，処理性能のばらつきを抑えることで，機密性を高められることが分かる．

5. 履歴に基づく処理ノード選択法

5.1. 選択アルゴリズム

処理ノードの選定の際，過去に利用した処理ノードの処理性能を管理ノードに保存しておく．新たに処理ノードの選定を行う際には，過去の処理結果を基に，高性能閾値以上の性能を持つノード (高性能ノード) から 4 割，低性能閾値以下の性能となるノード (低性能ノード) から 1 割，残りをランダムなノードとして利用する．このように，処理ノードの一部を過去の処理時間に基づいて選定することで，処理性能のばらつきを抑え，機密性の向上を図る．本稿では，機密性と高速性に関して，以下の条件でシミュレーションを行い，既存の方法と定量的に比較する．

5.2. 機密性に関する評価

シミュレーションは，表 1 の条件で行った．

シミュレーションの結果は図 2 のとおりである．利用している処理ノードの数は，既存の方法と比べ，約 5%減少し，機密性の向上が伺える．また，検定を行ったところ，有意水準 1%を満たし，有意差があるが示された．これにより，提案手法は，既存の方法と比べて

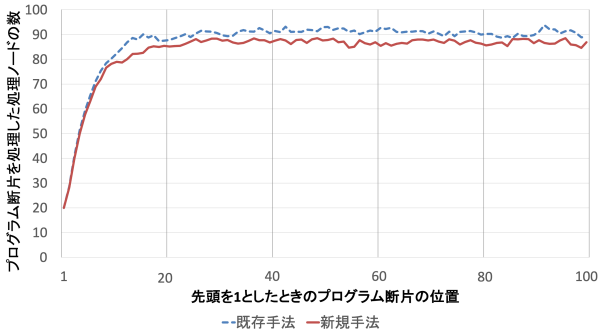

図 2: 断片ごとの処理ノード数

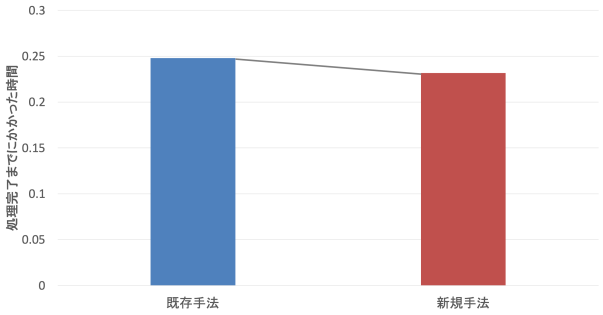

図 3: 処理完了までにかかる時間

機密性の向上させるという結果となった．

5.3. 高速性に関する評価

高速性に関するシミュレーションにおいても，機密性の場合と同様に表 1 の条件で行った．シミュレーションの結果は図 3 のとおりである．処理終了までにかかった時間は，既存の方法では約 0.248，新規手法では約 0.232 であり，約 6%の向上が見られる．また，検定を行ったところ，有意水準 1%を満たし，有意差があることが示された．

6. まとめ

本稿では，処理ノードの処理性能のばらつきを抑えることで，機密性が向上することを示し，その結果から処理ノードの処理性能を記録し，処理性能によって利用する割合を変えることで，機密性と高速性の両方を向上させられる手法を提案した．今後の課題として，保存対象となる処理ノード数に制限を設けるなど，より現実的な条件でのシミュレーションが挙げられる．

参考文献

[1] 田中祐生 遠藤慶一 樋上喜信 小林真也 (2017) “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” 情報処理学会第 79 回全国大会講演論文集