PBFT におけるクラスタ化を用いたビザンチン耐性の向上

Imorocing Byzantine Resistance Using Clustering in PBFT

岡田 鉄平[1]　　上山 憲昭[2]
Teppei Okada　　Noriaki Kamiyama
立命館大学大学院 情報理工学研究科[1]
Graduate School of Information Science and Engineering, Ritsumeikan University
立命館大学 情報理工学部[2]
College of Information Science and Engineering, Ritsumeikan University

1. はじめに

近年，取引を改ざん困難な状態で複数のコンピュータ間で共有して管理するブロックチェーンが注目を集めている．ブロックチェーンでは，新たなブロックを追加する際に台帳情報を参加者全員で共有するための合意形成が行われるが，中でも PBFT (practical byzantine fault tolerance) は，一部の組織内のみで使用されるコンソーシアム型のブロックチェーンで主に採用される．PBFT は故障や攻撃が発生したノード (ビザンチンノード) に対して耐性のあるアルゴリズムであり，ビザンチンノード数が全体の 3 分の 1 以下であれば正しく合意に達することができる．

一方，PBFT は 3 分の 2 以上の正常ノードが存在することが前提であるため，攻撃者が一定数以上存在すると合意形成が困難となる．既存研究 [1][2] では，クラスタリングを用いることでスループットを向上させる方式が提案されている．一方，クラスタ構成が静的で，動的な環境に対応できない点が課題であり，またビザンチン耐性の向上を目的としたクラスタ構成法は未検討である．

そこで本稿では，ブロックチェーンネットワークにクラスタリングを適用して攻撃者の場所を推定することで，ビザンチンノードに対する耐性をもつクラスタを構成する方式を提案する．

2. PBFT

PBFT ではクライアント，レプリカノード，プライマリノードで構成される．クライアントはトランザクションを生成してネットワークに送信し，レプリカノードはネットワーク内の各ノードを指す．プライマリノードは特定のレプリカノードであり，クライアントからトランザクションを受け取り，他のレプリカノードに転送する役割がある．

また，正確な合意を取るため，クライアントがプライマリノードにトランザクションを送信した後，pre-prepare フェーズ，prepare フェーズ，commit フェーズの三つの段階を通じて合意を達成する [3]．全体の 3 分の 2 のノードから commit メッセージを受け取ると，正しく合意できた旨を reply メッセージとしてクライアントに送信する．

3. 提案方式

本節では，提案方式の概要を説明する．まず全体で PBFT を実行し，合意が取れなければクラスタリングにより分割する．それぞれのクラスタ内で PBFT を実行し，さらにその結果を元にクラスタ間で PBFT を実行する．そのため少数派の意見を送信したクラスタを複数，マージすることで，多数派の意見を送信するクラスタ数の比率を高めることができ，全体として正しい合意形成が得られやすくなる．そこで合意が取れなかった場合は少数派の意見を送信してきたクラスタの攻撃者が多いと判断し，少数派のクラスタどうしを結合する．全体の合意が正しく形成されれば終了する．

提案方式では，攻撃者が全体の 3 分の 1 以上存在していても，その影響を受けずに合意形成できることが期待される．

4. 性能評価

提案方式を計算機シミュレーションにより評価する．ノード数を 90 とし，攻撃者数を 0 から 90 まで変化させ，(a) 合意に達した割合および (b) 発生トラフィック量を図 1 に示す． Barabasi-Albert (BA) モデルを用いて生成したネットワークトポロジを用いて，提案方式と従来の PBFT，k-means 法を適用した PBFT (k=4, 7, 10, 15) を比較した．

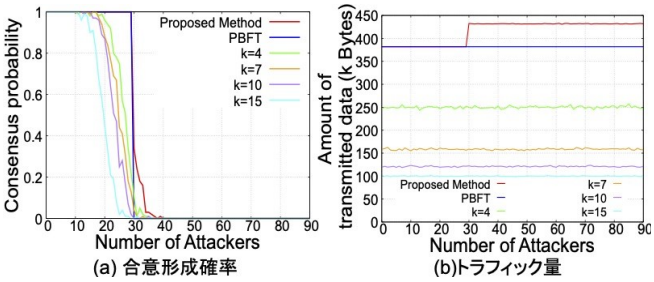

図 1: 攻撃ノード数に対する特性

図 1(a) より，提案方式の合意形成確率が最も高く，攻撃者数が全体の最大 44%存在していても正しく合意形成できることが確認できる．これは攻撃者が多いクラスタが集約され，正しい結果を得るクラスタの比率が増加するためである．

一方，既存の PBFT に加え，クラスタリング後の PBFT によるトラフィックが発生するため，図 1(b) より，提案手法のトラフィック量が最も多くなることが確認された．今後は，トラフィック量を抑え，さらに合意形成確率を上げる手法を考案する予定である．

謝辞本研究成果は JSPS 科研費 21H03436 と 21H03437 の助成を受けたものである．ここに記して謝意を表す．

参考文献

[1] R. M. Othmen, et al., Simulation of Optimized Cluster Based PBFT Blockchain Validation Process, IEEE ISCC 2023

[2] A. J. Al-Musharaf, et al., Improving Blockchain Consensus Mechanism via Network Clusters, BICITS 2021

[3] M. Castro, B. Liskov, Practical byzantine fault tolerance, OSDI 1999