ブロックチェーンのビザンチン耐障害性の動的クラスタリングによる強化

Improving Byzantine Fault Tolerance in Blockchain via Dynamic Clustering

岡田 鉄平[1]　　上山 憲昭[2]　　藤原 明広[3]
Teppei Okada　　Noriaki Kamiyama　　Akihiro Fujihara
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
千葉工業大学 工学部[3]
Faculty of Engineering, Chiba Institute of Technology

1. はじめに

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，合意形成が必要となる．その中でも PBFT (Practical Byzantine Fault Tolerance) [1] は，主にコンソーシアム型ブロックチェーンにおいて広く採用されているアルゴリズムである．PBFT は，故障や攻撃によるビザンチンノードに対する耐性を備え，全ノードのうちビザンチンノードが 3 分の 1 未満であれば正しい合意形成が可能である．しかしながら，PBFT は 3 分の 2 以上の正常ノードが存在することを前提としており，一定数以上の攻撃者が存在する場合，合意形成が困難になるという課題がある．

著者らは以前，ブロックチェーンネットワークにクラスタリング手法を適用し，攻撃者の位置を推定することで，ビザンチンノードに対する耐性を持つクラスタを構築する方式を提案した [2]．しかし，この方式では合意形成確率の向上が十分でなく，また冗長な通信が原因でトラフィック量が増加するという課題が生じた．

本稿では，[2] の方式を改良し，合意形成確率のさらなる向上とトラフィック量の削減を目指した新たな方式を提案する．

2. 提案方式

本節では，提案方式の概要について説明する．

1. k-means 法を適用し，ネットワークを複数のクラスタに分割
2. 各クラスタ内で PBFT を実行し，クラスタごとに一時的な合意を形成
3. クラスタ内で得られた結果を基に，クラスタ間で PBFT を実行
4. コンセンサスが得られない場合，少数意見を送信したクラスタに攻撃者が多数存在すると判断し，すべての少数意見のクラスタを一度にマージ
5. コンセンサスの形成に成功した場合，その旨をネットワーク全体に共有し，終了

提案方式は，[2] の方式と比較して以下の点で大きく異なる．提案方式では最初の PBFT を実行せず，段階的に PBFT とマージを進めるのではなく，これらを一度に実行する．この改良により，合意形成の正確性を維持しながら，トラフィック量を大幅に削減することが可能となる．

3. 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，それぞれの場合に対して合意に達した割合およびトラフィック量を図 1 に示す．ネットワークトポロジは Barabasi-Albert (BA) モデルを採用し，提案方式と従来の PBFT，および k-means 法を適用した PBFT (k=7, 10, 15)[2] を比較した．また，攻撃者は特定の領域に集中的に配置し，ノード間の位置関係が近いものを同一クラスタに分類できるように k-means 法を適用した．

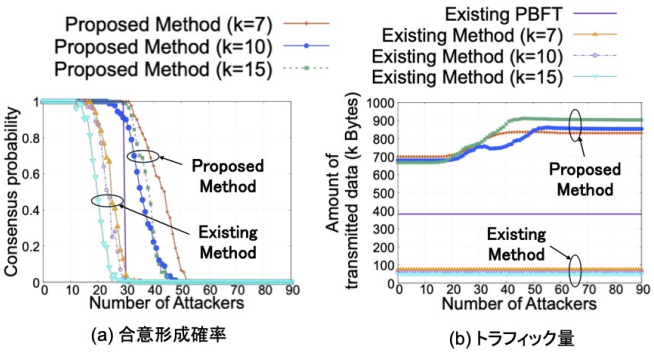

図 1: 合意形成確率および通信トラフィック量の比較

図 1(a) より，提案方式の合意形成確率が最も高くなり，攻撃者数が全体の最大 5/9 以上存在していても正しく合意形成す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，全体として攻撃者の割合が減少するためである．しかし，攻撃者の数が 25~30 人（全体の 3 分の 1 未満）の場合にはコンセンサスに達しない場合がある．これは最初のクラスタリング結果によるもので，攻撃者が過半数を占めるクラスタが全体の半分以上を占めることがあるためである．

一方図 1(b) より，提案方式のトラフィック量は従来の PBFT よりも多いが，既存方式 [2] と比較して，マージや PBFT の実行頻度が減少したため，トラフィック量を削減できたことが確認できる．

謝辞本研究成果は JSPS 科研費 23K11086，23K21664，23K28078 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] M. Castro, et al., “Practical byzantine fault tolerance,” in Proc. of third symposium on Operating systems design and implementation (OSDI ’99), 1999, pp. 173-186.

[2] 岡田 鉄平，上山 憲昭，PBFT におけるクラスタ化を用いたビザンチン耐性の向上, 電子情報通信学会ソサイエティ大会, N-2-05，2024 年 9 月