PBFTにおけるクラスタ化を用いたビザンチン耐性の向上

立命館大学

岡田鉄平 上山憲昭

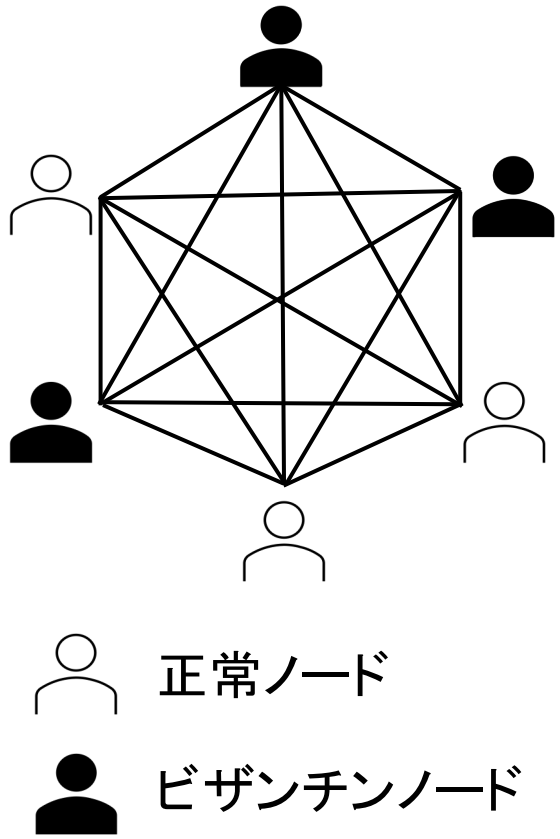
研究背景 (1/2)

- ブロックチェーン
  - 取引を改ざん困難な状態で複数のコンピュータ間で台帳上で共有して管理
  - パブリック型
    - 管理者が不在
    - ex. Bitcoin, Ethereum
  - コンソーシアム型，プライベート型
    - 管理者が存在
    - ex. Hyperledger
- 合意形成
  - 新たなブロックやトランザクションが作成された際に参加者全員で検証
  - 改ざん可能性のあるトランザクションを検知・排除
  - コンソーシアム型ではPBFT (practical byzantine fault tolerance)が主に採用

研究背景 (2/2)

- PBFT
  - 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
  - ビザンチンノード数が全体の3分の1未満であれば正しく合意に達することが可能

- デメリット
  - ビザンチンノード数が3分の1以上存在
    →正しい合意形成が困難



研究目的

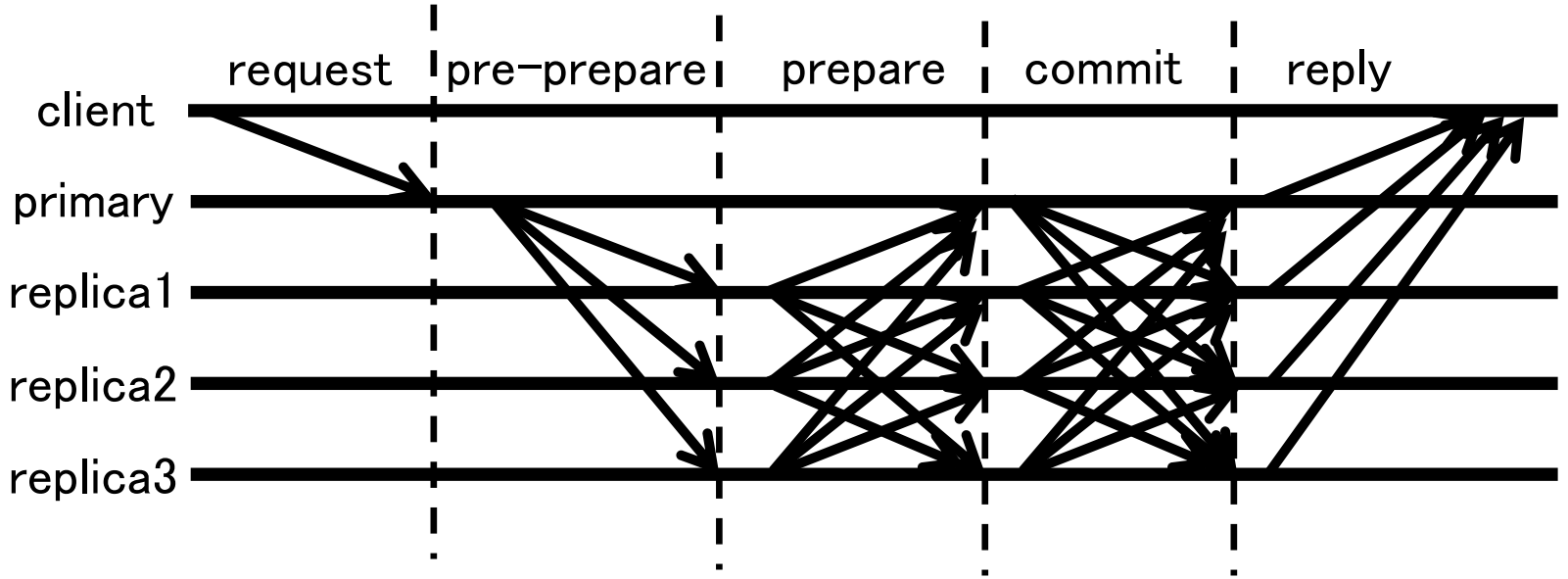
- PBFT
  - ビザンチンノード数に合意が左右

- クラスタリングにより，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

- k−means法でトポロジを分割し，PBFTによりクラスタ内，クラスタ間で合意を形成
  - 少数派の意見を送信するクラスタを合成

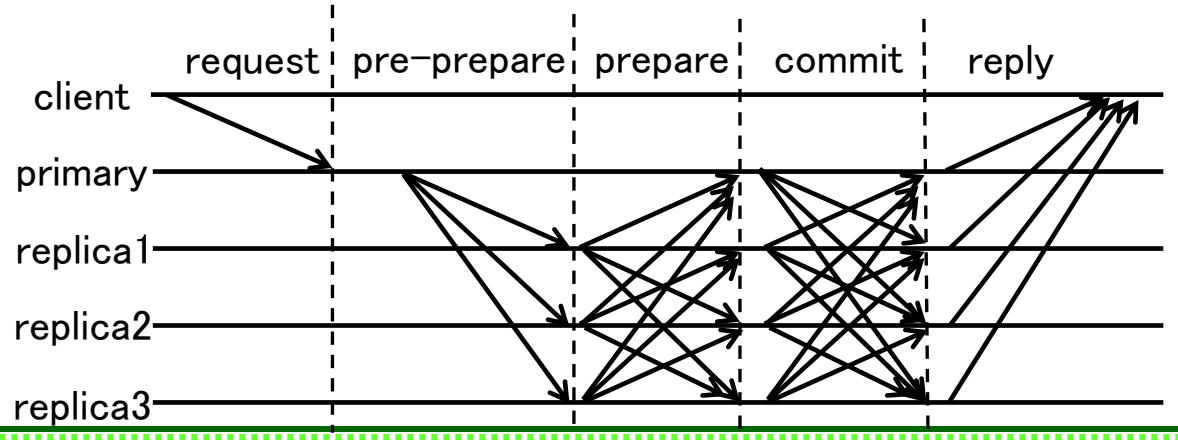
PBFT（1/2）

- 3種類のエンティティにより構成
  - クライアント
    - トランザクションを生成してネットワークに送信
  - レプリカノード
    - コンセンサスに参加するノード
  - プライマリノード
    - 特定のレプリカノード
    - 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



PBFT（2/2）

- 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後，3つの段階を通して合意形成
  - pre-prepareフェーズ
    - プライマリノードが他のレプリカノードにトランザクションを転送
    - 各ノードはトランザクションの正当性を検証後，他ノードに結果をブロードキャスト
  - prepareフェーズ
    - レプリカノードは，検証した結果がプライマリノードの検証結果と一致していることを確認
    - 他のノードにブロードキャスト
  - commitフェーズ
    - prepareフェーズで受け取ったメッセージに同意する場合，commitメッセージを他のノードに送信
- 全体の3分の2のノードからcommitメッセージを受信
  - 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



提案方式

1. 全体でPBFTを実行

2. 合意が形成できなければ，ネットワークにk-means法を適用

3. それぞれのクラスタ内でPBFTを実行

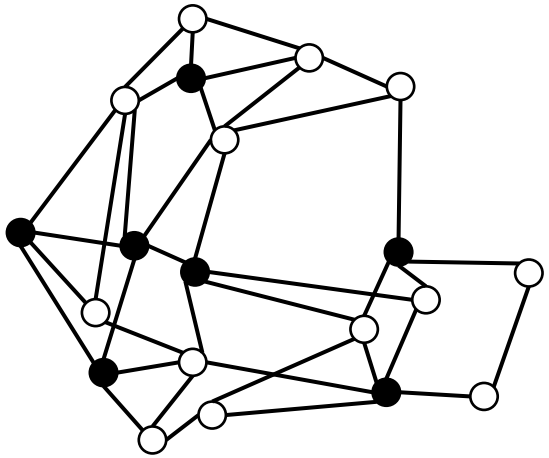
4. クラスタ間でPBFTを実行

5. 合意が取れなかった場合，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
   - 少数派のクラスタ同士を合成

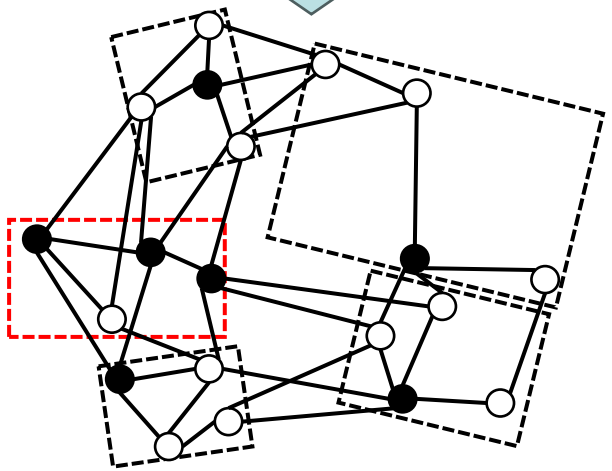
6. 全体の合意が正しく形成されれば終了

提案方式（例）

- 上図（提案方式適用前）
  - 20ノードのうち，7ノードがビザンチンノード
  - →ビザンチンノードが全体の3分の1を超えているため，PBFTを実行しても合意形成不可能



- 下図（提案方式適用後）
  - クラスタリングの結果，5つのクラスタが発生
  - ビザンチンノードの割合が3分の1未満のクラスタは4つ
  - →クラスタ間でPBFTを実行すると，合意に達する

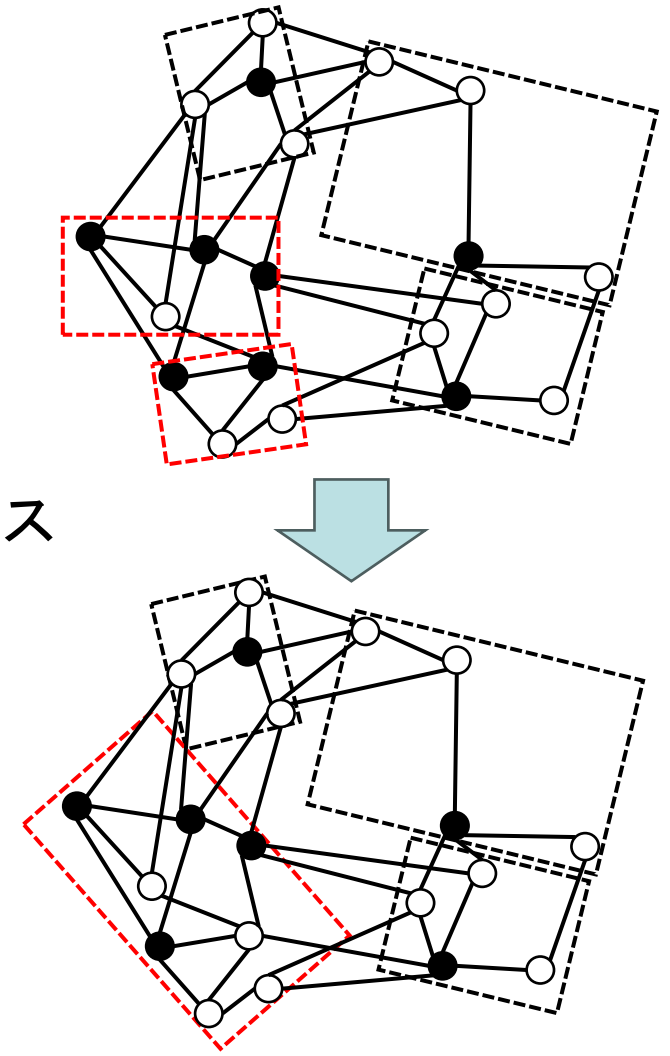


○ 正常ノード

● ビザンチンノード

クラスタの合成

- 上図
  - ビザンチンノードの割合が3分の1未満のクラスタが3つ
    - 合意形成不可能
  - 少数派のクラスタ（赤点線)を合成
- 下図
  - 4つのクラスタのうち，ビザンチンノードの割合が3分の1未満のクラスタが3つ
  - 正常に合意を形成することが可能



性能評価

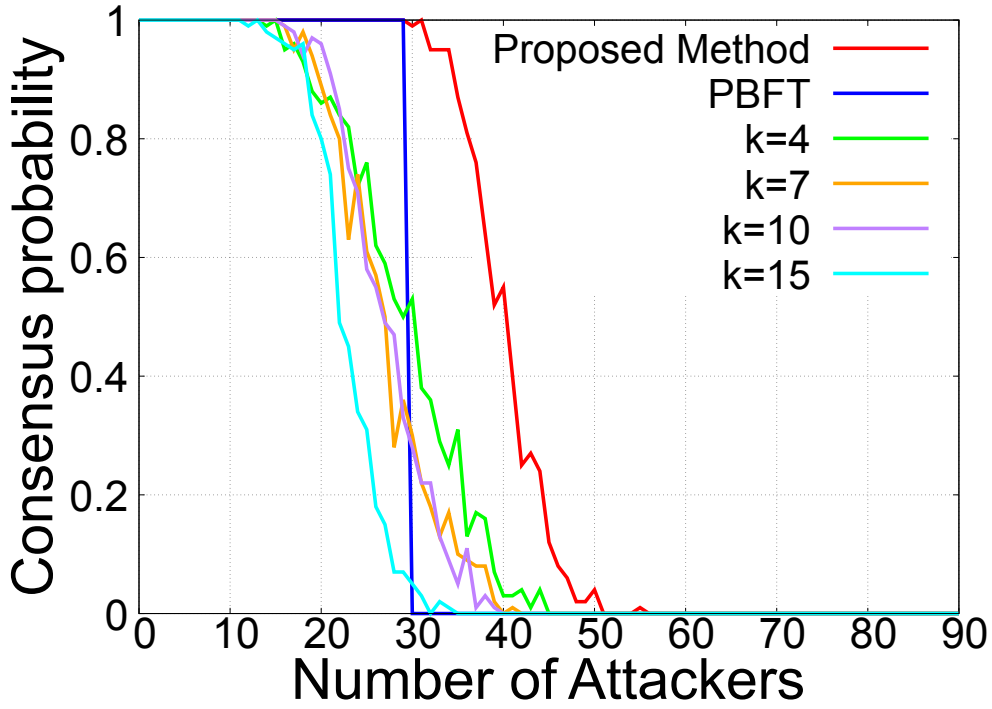
- 計算機シミュレーションにより評価
  - 合意に達した割合
    - 100回中合意に達した回数をカウント
  - 発生トラフィック量

シミュレーション条件

- ノード数: 90
  - 攻撃者数を0から90まで変化
- ネットワークトポロジ: Barabasi–Albert (BA) モデル
- 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

合意形成確率

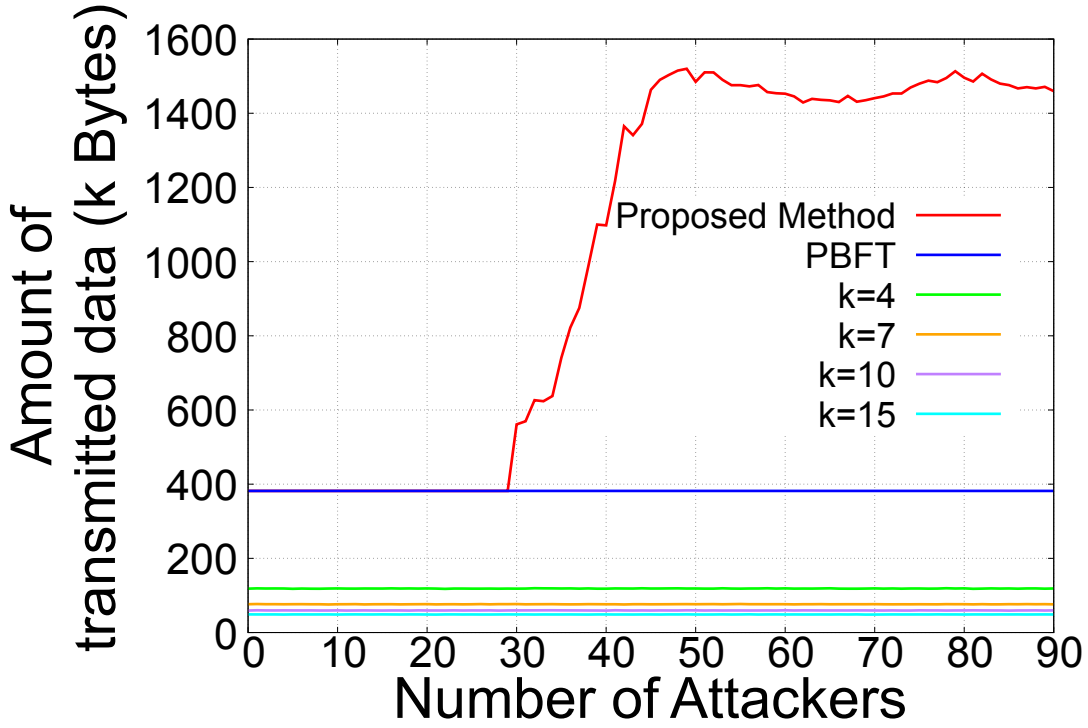
合意形成確率



- 提案方式の合意形成確率（赤)が最も高
  - 攻撃者の多いクラスタが集約
  - →正しい結果を得るクラスタの比率が増加

トラフィック量

トラフィック量



- トラフィック量は，提案方式が最も多
  - クラスタリング後のPBFTによるトラフィックが発生
  - PBFTではデータがブロードキャスト
    - →トラフィック量が増加

まとめ

- コンソーシアム型のブロックチェーンで主に使用されるPBFTにおいて，k-means法を適用する手法を提案
  - 攻撃者が多いクラスタを分割，合成することで正しく合意を形成することが可能

- 今後の予定
  - ネットワーク全体の通信量を削減
  - クラスタを最適化するアルゴリズムを検討