九州工業大学 情報工学部 情報・通信工学科 2022 年度 卒業論文 概要

コース	情報通信ネットワーク	指導教員	川原 憲治
学生番号	192C1079	氏　　名	菅野 龍哉

論文題目	PoA ブロックチェーンに基づく自律分散無線アクセス共用網における Authority ノード機能の代替方法に関する研究

1　背景

移動端末の普及，公衆無線 LAN サービスの拡大により無線 LAN アクセスポイント (AP) の稠密設置が予想され，管理者の異なる AP の共用が可能な Proof of Authority(PoA) に基づくブロックチェーン技術を適用した無線 AP 共用網が検討されている. 本研究では，通常 AP が Authority ノードを兼任することで配置コストの削減を図ることを前提に，Authority ノード機能の実現方法や，同一管理下の AP 群における Authority ノード機能の代替方式について検討する.

2　自律分散無線 AP 共用網 [1]

Bitcoin ベースの実装を想定し，AP をフルノードとして共用網への自律的な参加/離脱を実現し，接続端末の情報も含めて分散管理する. 端末は軽量ノードとして自身の契約・接続情報のみを保持し，共用網の利用時に契約状況に関わらず近接 AP に対して接続認証トランザクション (TX) を送信，認証後ブロックに格納される AP との接続/切り替えを可能とする.

3　PoW と PoA[2]

共用網への接続端末が増加すると，参加/離脱の頻度が高くなり，ビットコインのブロック生成手法である Proof of Work(PoW) では任意の生成者による計算と検証に時間がかかるため，迅速な接続や切り替えに対処するのは難しいと考えられる．一方，PoA では少数の Authority ノードがブロック認証するため，ブロック生成時間を削減しリアルタイムな情報共有を可能とする. しかし，Authority ノードが固定の場合，セキュリティ上問題がある. また，故障時にブロック生成ができなくなる.

4　Authority ノード機能の代替方式

Authority ノード機能を通常 AP に兼任させる代替方式を提案する.

4.1　Authority ノード機能の実現方法

Authority ノードの実現方法を図 1 に示す. ここで，各管理下 AP を色の違いで示している.

1. Authority ノード機能の起動：各管理下で起動した AP をまとめたグループを Authority ノード群とする
2. 他の Authority ノードから TX を受信：管理下 C の AP が代替する場合，他の管理下 A,B,D の Authority ノードが持つ TX を受信
3. 新たな Authority ノード群を構成

4.2　Authority ノード機能の交代方法

4.2.1　通常時：スケジューリング

Authority ノード機能を行う AP はあらかじめスケジュールされた順番で交代

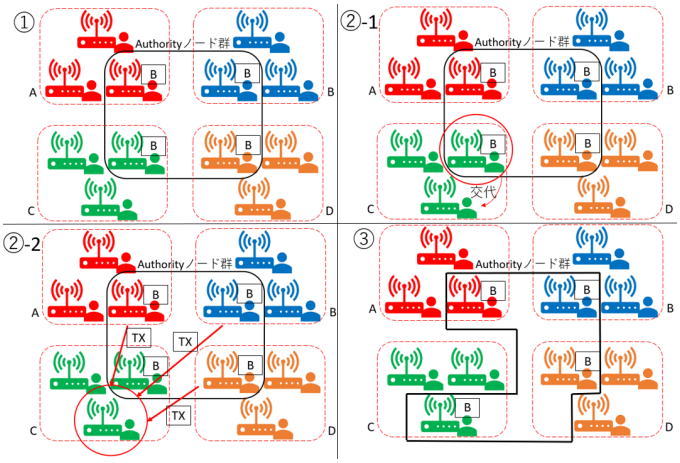

図 1. Authority ノード機能の実現方法

4.2.2　緊急時

Authority ノード機能を有する AP が停止した場合，ブロック生成ができなくなるため，その検知と Authority ノード機能の代替が必要となる.

不具合の検知は同一管理下の AP に対して行う.

1. AP は近接 AP に対して定期的に ping を送信
2. 近接 AP からの応答がないと不具合を検知
3. 不具合をその他の AP にブロードキャスト

代替方法には Proof of Elapsed Time(PoET)[3] を活用する.PoET は，Intel Corporation により開発されたコンセンサスアルゴリズムで，以下の手順で任意の AP から Authority ノードを選出する.

1. Intel が各 AP に証明書とタイマーを与える
2. 各 AP にランダムな待機時間が与えられる
3. 待機時間が最短の AP は Authority ノード機能を起動
4. 起動した AP はブロック生成権を得て，Authority ノード群を構成

5　まとめと今後

PoA ブロックチェーンに基づく共用網において，Authority ノード機能の代替方式について検討した.

参考文献

[1] 青山寛樹, 川原憲治, ”ブロックチェーン技術を適用した 自律分散無線アクセス共有網の検討”, 電子情報通信学会 2019 総合大会, B-7-42.

[2] Nurin Izzati Binti Jafri,　川原憲治, ”ブロックチェーン技術を適応した自律分散無線アクセス共用網における効率的なトランザクション処理に関する研究”, 九工大 2021 卒業論文.

[3] Jake Frankenfield, Proof of Elapsed Time (PoET) Definition, Purposes, Vs. PoW, https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp, 2022.