電子情報工学科 (川原研究室)

学生番号	19232207	氏名	Nurin Izzati Binti Jafri
論文題目	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		

1 はじめに

近年の移動端末の普及により，公衆無線 LAN サービスの拡大と無線 LAN アクセスポイント（AP）の稠密設置が予想される．そこで，管理者の異なる AP の共用を可能とする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，端末と AP の接続や切り替えを迅速に行うための認証プロセスとブロック生成手法について検討する．

2 自律分散無線 AP 共用網 [1]

自律分散無線 AP 共用網ではビットコイン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，接続端末に関する情報も含めて分散管理する．一方，接続端末は軽量ノードとして自身の契約・接続に関する情報のみを保持する．端末は共用網を利用する際に AP に対して接続認証のためのリクエスト TX を送信，ブロックに格納されることで AP との接続/切り替えを行う．

3 共用網における端末認証とブロック生成手法

接続端末が増加すると，共用網における参加/離脱の頻度は非常に高くなり，ビットコインにおけるブロック生成手法 Proof of Work(PoW)[2] では任意の生成者による複雑な計算と正当なブロックの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困難であると考えられる．Proof of Authority(PoA) では少数特定（Authority）ノードがブロックを認証し，ブロック生成時間を短縮可能なため，共用網におけるリアルタイムな端末-AP の接続/認証のため，PoA を前提とした端末における接続要求のリクエスト TX と AP における接続応答のレスポンス TX を定義し，認証プロセスとブロック生成方式を提案する．

3.1 端末認証

異なる管理者/キャリアが提供する AP 群で構成される共用網を前提とする．端末が共用網に参加する際，契約している管理者の AP が認証をする必要がある．そこで図 1 に示す認証手法を提案する．

1. 端末 T（管理者 A）が近接 AP にリクエスト TX を送信
2. (a) 近隣 AP（管理者 B）は端末 T が管理者が異なると判断，接続要求リクエスト TX をブロードキャスト（転送）
   (b) 管理者 A の AP が端末 T の接続要求リクエスト TX を認証し，認証リクエスト TX を近隣 AP や Authority ノードに送信
3. 近隣 AP は端末の接続 AP を示すレスポンス TX を端末に送信

共用網の AP 群に管理者を持たない端末が参加する際，近隣 AP からブロードキャストされた接続要求リクエスト TX の認証ができないため，近隣 AP でタイマーを設定し，タイムアウトが発生したら，端末に認証失敗を示すレスポンス TX を送信する．

3.2 PoA によるブロック生成方式

PoA ではブロック生成権を持つ Authority ノードが新たに必要で，共用網の構成 AP はブロック生成に関与しない Non-Authority ノードとする．正式なブロックと認定するには 51% 以上の Authority ノードの署名が必要となる．3 つの管理者の Authority ノードが存在し，管理者 C の Authority ノードがブロック生成する場合の例を図 2 に示す．

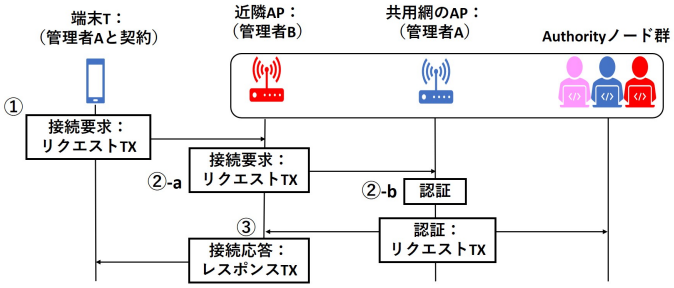

図 1: 端末-AP の認証

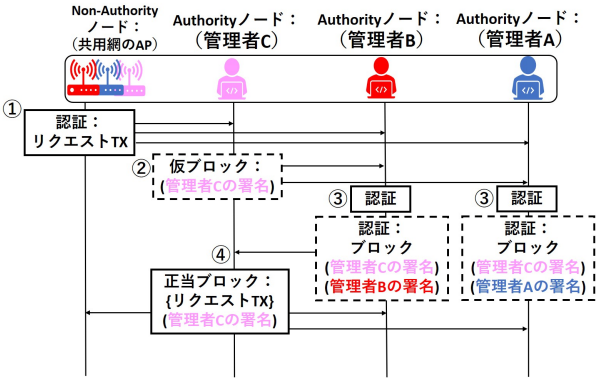

図 2: PoA によるブロック生成方式

1. 認証リクエスト TX を Authority ノード A,B,C が受信
2. Authority ノード C はリクエスト TX をブロックに取り込み，自身の秘密鍵で署名して，他の Authority ノードに送信
3. Authority ノード A/B はブロックの有効性を検証，正当性であれば，自身の秘密鍵で署名，ブロードキャスト
4. Authority ノード C が 51% 以上（2 ノード）の Authority ノードが署名したブロックを受信すると，正式なブロックとして共用網全体にブロードキャスト

4 まとめ及び今後の方針

自律分散無線 AP 共用網においてリアルタイム性を提供するため，PoA を実装する共用網を提案し，端末認証手法とブロック生成手法の設計をした．今後は，テストベッドネットワークにおける PoA 技術を適用した自律分散無線アクセス共用網の実現性を検証する．

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] 樋野貴文，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における AP-端末間チャネル構築方式に関する研究”，九工大 2019 年卒業論文.