九州工業大学大学院情報工学府　先端情報工学専攻　電子情報工学専門分野（川原研究室）

| 学生番号 | 21676125 | 氏　名 | NURIN IZZATI BINTI JAFRI |
|---|---|---|---|
| 論文題目 | PoA ベースのブロックチェーン技術を適用した自律分散無線 AP 共用網に関する研究 | | |

## 1　はじめに

近年の移動端末の普及により，公衆無線 LAN サービスの拡大によるアクセスポイント (AP) の稠密設置が予想され，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 AP 共用網が提案されている．本研究では，端末-AP 間の認証や接続/切り替えを迅速に行うための認証処理と Proof of Authority(PoA) ベースのブロック生成手法を検討する．

## 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ことで AP との接続/切り替えを可能とする．

しかし，Proof of Work(PoW) によるブロック生成手法では正式なブロック検証に時間を要し，接続端末が増加すると参加/離脱の頻度が非常に大きくなり，迅速な接続/切り替えに対処するのは困難であると考えられる．

## 3　PoA を適用した自律分散 AP 共用網の提案

PoA では少数の特定 (Authority) ノードがブロック認証するため，ブロック生成時間が短縮可能となる．本研究では AP 管理者毎の Authority ノード設置を想定し，リアルタイムな端末-AP 間の接続/切り替えの端末認証とブロック生成手法を提案する．

- 端末：AP 共用網外に存在し，AP に対する要求，応答は「メッセージ」形式で通信
- AP：端末からの接続要求などにより，「TX」を生成
- Authority ノード:各管理者の Authority ノードにより群を構成してブロック生成とし，契約端末の共用網参加認証のための [デジタル証明書]，[端末情報]，[端末情報] のハッシュ値 [TH] を発行

### 3.1　Authority ノードと AP による端末認証の概要

[1] では端末は契約サービス提供者の管理者識別子を，各 AP は共用網に参加する全提供者の管理者識別子を有すると仮定し，AP における端末認証はそれらの比較のみで行うためセキュリティ面が不安視される．本研究では端末は契約管理者の Authority ノードの審査に基づく [デジタル証明書]，[端末情報]，[TH] の保持を前提とし，全 Authority ノードの公開鍵を有する各 AP において検証することで，セキュリティ面の強化を可能とする．Authority ノード群では期間毎にブロック生成する Primary が選択され，その他はブロック検証のみ行う．

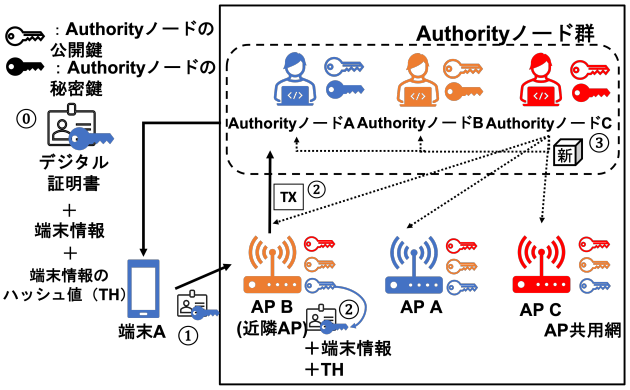


図 1. PoA ベースの端末認証とブロック生成手法

図 1 に端末 A が近隣 AP(AP B) に接続するものとし，Primary(Authority ノード C) がブロック生成を示す．

0. Authority ノード A：秘密鍵で署名した端末 A の [デジタル証明書]，[端末情報]，[TH] を事前に送信
1. 端末 A：AP B に [デジタル証明書] と [端末情報] と [TH] を含む接続要求を送信
2. AP B：端末認証が成功すると，接続 TX を生成し Authority ノード群に送信
   (a) [デジタル証明書] と [TH] により，[TH] の署名者の公開鍵を導出
   (b) 保有している Authority ノード A の公開鍵と導出された公開鍵が一致であれば，②-c に進む
   (c) [端末情報] をハッシュ化し，生成したハッシュ値と [TH] が一致であれば，端末認証が成功
3. Authority ノード C(Primary)：TX をブロックに取り込み，全ネットワークに伝搬

### 3.2　PoA によるブロック生成時間の検証

PoA では少数の Authority ノードにより難易度を低く設定し計算量を抑えてブロック生成速度の向上が可能となる．そこで 3.1 の端末認証と PoA によるブロック生成手法が可能なブロックチェーンネットワークのプラットフォームである Hyperledger Besu にて実装 (Authority ノード数：3,AP 数：3, 端末数：1) したところ，ブロック生成時間は 15 秒となった．

## 4　まとめ及び今後の方針

ブロックチェーン技術を適用した自律分散無線 AP 共用網において PoA に基づくセキュリティ面を考慮する端末認証とブロック生成手法を提案し，実装を通してリアルタイムな端末接続を提供可能であると示された．

## 参考文献

[1] 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”,2021 総合大会，B-7-12.