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	19676128	氏　名	樋野　貴文
論文題目	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用網における チャネル構築とトランザクション設計に関する研究		

1　はじめに

近年の移動型端末の普及により，公衆無線 LAN サービスの拡大と無線 LAN アクセスポイント (無線 AP) の稠密設置が予想される．そこで，管理者の異なる無線 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．本研究では共用網における端末認証手順と必要なトランザクション (Tx) について提案し，実環境に実装して確認する．

2　自律分散無線アクセス共用網 [1]

ブロックチェーン技術を適用した共用網ではビットコインベースの実装を想定し，共用網を構成する 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，接続端末に関する情報も含めて分散管理する．一方で，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．しかし，フルノード-軽量ノード間 Tx の確定には時間を要し，リアルタイム性を要求する端末の認証/接続が困難であると考えられる．

3　受付 AP への端末認証・接続手順（図 1）

端末認証/接続の高速化と接続情報共有のため，端末-受付 AP 間にオフチェーンチャネルを構築し，端末の管理者/契約キャリアに属する AP の共用網における存在状況を受付 AP で局所的に確認後，Tx としてブロードキャストすることを提案する．

3.1　接続要求と端末認証 (メッセージ形式)

1. 接続要求：近接 AP へ端末情報送信
   端末は「親公開鍵」「子公開鍵」「親チェーンコード」をビットコインメッセージ形式で受付 AP へ送信．
2. 端末認証
   受付 AP は「親公開鍵」「親チェーンコード」と，自身が有する管理者識別子（構成 AP を提供する管理者/キャリアの識別値）群から複数の公開鍵を導出し「子公開鍵」と比較し一致する場合に端末を接続．

3.2　接続情報の共有 (トランザクション定義)

受付 AP で端末認証が成功すると，接続許可と収容 AP を示す Tx を作成し他 AP へブロードキャストする．

4　設計トランザクションの有効性検証

提案する Tx/手順の有効性確認のため図 2 のテストベッドネットワークにて実験する．端末/AP は bitcoin-core クライアントとし，端末:1 は契約関係にない近接の AP:2 を会して Web サーバからデータ取得を行う．図 3 に AP:2 におけるメッセージ交換/Tx 作成ログを示す．

- 1-9 行目はメッセージによるハンドシェイク

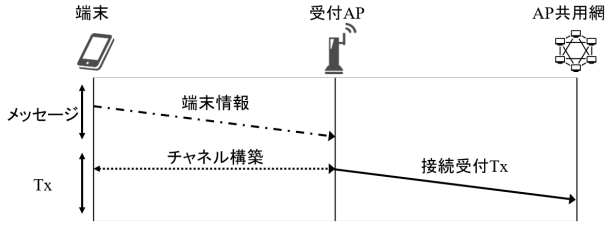

図 1. 端末の認証手順

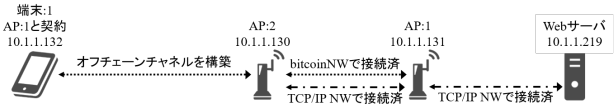

図 2. 実験環境のトポロジ

```
 1 2021-02-02T08:17:25Z Added connection peer=2
 2 2021-02-02T08:17:25Z connection from 10.1.1.225:37362 accepted
 3 2021-02-02T08:17:25Z received: version (104 bytes) peer=2
 4 2021-02-02T08:17:25Z sending version (103 bytes) peer=2
 5 2021-02-02T08:17:25Z send version message: version 70016,
   blocks=101, us=[::]:0, peer=2
 6 2021-02-02T08:17:25Z sending verack (0 bytes) peer=2
 7 2021-02-02T08:17:25Z sending sendaddrv2 (0 bytes) peer=2
 8 2021-02-02T08:17:25Z receive version message: /bitcoinrb:0.0.20/:
   version 70016, blocks=0, us=10.1.1.132:18444, peer=2
 9 2021-02-02T08:17:25Z received: verack (0 bytes) peer=2
10 2021-02-02T08:17:25Z received: mw7ayBpjq4NT (0 bytes) peer=2
11 2021-02-02T08:17:25Z Unknown command "mw7ayBpjq4NT" from peer=2
12 2021-02-02T08:17:25Z received: aNfVtMyAezVp (0 bytes) peer=2
13 2021-02-02T08:17:25Z Unknown command "aNfVtMyAezVp" from peer=2
14 2021-02-02T08:17:25Z received: kkdQmXS84b (0 bytes) peer=2
15 2021-02-02T08:17:25Z Unknown command "kkdQmXS84b" from peer=2
16 2021-02-02T08:17:25Z received: 87201dc8210c (0 bytes) peer=2
17 2021-02-02T08:17:25Z Unknown command "87201dc8210c" from peer=2
18 2021-02-02T08:17:26Z [syuji] AddToWallet
   b92658d5f4485117b53c64bd4a3ce4b5eb718153a9a45265b2f97c7e4284a6ca new
19 2021-02-02T08:17:26Z Transaction created
20 2021-02-02T08:17:41Z sending inv (37 bytes) peer=2
21 2021-02-02T08:17:41Z received getdata for: tx
   b92658d5f4485117b53c64bd4a3ce4b5eb718153a9a45265b2f97c7e4284a6ca
   peer=2
22 2021-02-02T08:17:41Z sending tx (82 bytes) peer=2
```

図 3. AP2 におけるビットコインログ

- 10-17 行目は端末認証のための情報送信
- 18-22 行目が接続情報共有のための Tx 送信

に相当する．以上から端末:1 は AP:2 に認証され接続を確立し TCP 通信が可能となる．

5　まとめ

無線アクセス共用網において，リアルタイム性を提供する端末認証/接続のための Tx を提案し端末認証手法を実装した結果，契約状況の異なる AP への接続と共用網を介したデータ通信を可能とすることを示した．

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-7-42，2019 年 3 月．

研究業績

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用網におけるチャネル構築とトランザクション設計に関する研究”, 電子情報通信学会 2021 総合大会，2021 年 3 月発表予定．