電子情報工学科 (川原研究室)

学生番号	17232207	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 AP-端末間チャネル構築方式に関する研究		

1 はじめに

近年，移動型端末の普及により公衆無線 LAN サービスは拡大し，各無線 LAN アクセスポイントにおける通信量が増加しているため，今後も AP の稠密設置が予想される．そこで管理者の異なる AP 同士を共用管理することで，データの収容性能を向上させる AP 共用ネットワークが必要とされており，ブロックチェーンを用いた自律分散無線アクセス共用システムが提案されている [1].

本研究では，上記の無線アクセス共用システムにおいて AP-端末間の接続方法について着目し，ノードタイプに依存しない論理的な通信路 (チャネル) の構築手法について示す.

2 現状のチャネル構築技術

2.1 ノードタイプ

ブロックチェーンシステムにおけるノードは大きく分けて 2 種類が存在する．1 つがブロックチェーンの全取引データを保持するフルノード，もう 1 つが自身に関する取引データのみを持つ SPV(Simplified Payment Verification) ノードである．SPV ノードはフルノードに比べデータ量が少ないため，スマートフォン等の軽量デバイスで用いられる.

2.2 オフチェーン

2 ノード間の取引内容はトランザクションと呼ばれ，オフチェーンとはブロックチェーン外でトランザクションの交換を行う技術である．これによって複数回のトランザクションを集約し，ブロックへ取り込むことで手数料を削減したり，第三者によるトランザクション検証を軽減することでトランザクションの高速な交換が期待できる.

3 提案手法

共用網を構成する AP はフルノードと定義し，P2P ネットワークを形成して各 AP の情報をブロックに格納する．一方で共用網の利用端末は SPV ノードと定義し，軽量機構のみを持ち，キャリアとの契約情報に関わらず接続する AP との間にチャネルを構築して，AP 利用認証やデータ取得を行うことになる．しかし，従来のチャネル構築手法では SPV ノードはフルノードを完全に信頼しなければフルノードとの間でチャネルを構築できない.

そこで本研究では，図 1 に示すような AP-端末間のチャネル構築手法を提案する.

3.1 データリンクレイヤ

まず，共用網における端末からの利用要求となるリクエストトランザクションを含むフレームを任意の AP で受信する必要がある．その手順を以下に示す.

1. 端末:T は接続を要求するリクエストトランザクションを作成し，フレームに組み込む.
2. リクエストフレームを近隣 AP へ送信.
3. AP は受信したフレームからリクエストトランザクションを取り出し，ブロックチェーンレイヤへ渡す.

3.2 ブロックチェーンレイヤ

フレームを受信した AP のブロックチェーンレイヤにおいて認証プロセスが実行される．以下に手順を示す.

1. リクエストトランザクションを受け取った AP(初期接続の場合はフレームを受け取った AP) は，端末の利用権を確認するためにトランザクションを検証する.

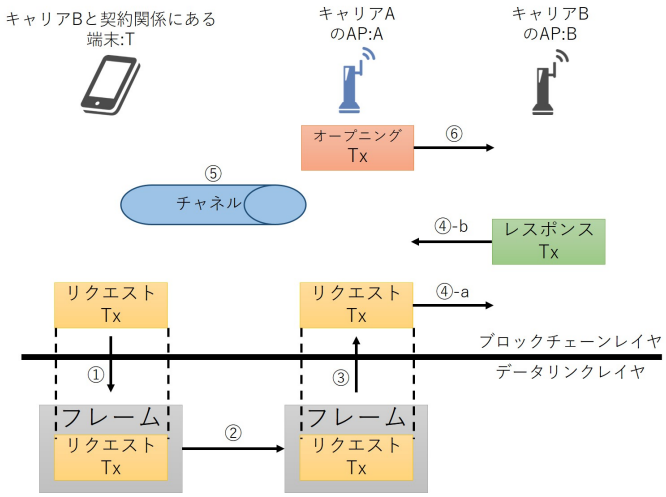

図 1: 提案手法

a 検証失敗
隣接 AP(図中 AP:B) へリクエストトランザクションをブロードキャストする.

b 検証成功
検証結果を含んだレスポンストランザクションをフレームを受信した AP(図中 AP:A) へ返送する.

2. 検証成功を受信した AP:A は端末:T が共用網の利用権を持つと認識し，AP:A と端末:T 間でチャネルを構築する.
3. AP:A は端末:T を収容したことを他の AP へ通知するため，オープニングトランザクションを作成しブロードキャストする.

以上により端末:T は AP:A との間でチャネルが構築され，共用網が利用できるようになる．この提案手法ではフルノードとして機能する AP 側で端末の信頼性を検証することで，ノードタイプに依存しないチャネル構築が可能となる.

4 データリンクレイヤにおけるフレーム認証

AP-端末間のフレーム送信がセキュリティ面の課題として挙げられる．今回提案手法において各 AP は，契約の有無によらず様々な端末からのフレーム受信を許容し，トランザクションを検証しなければならない．そのためフレームの大量送信による DoS 攻撃や，フレームにファームウェアを仕込まれるといった脆弱性が挙げられる．これを解決するためには AP におけるで SIM カードを用いた認証や，フレーム送信に手数料を課すなどの対策が必要となる.

5 まとめ

本研究では，ノードタイプに依存しない AP-端末間のチャネル構築手法について提案し，そのために必要となるトランザクションについて定義した．今後は手法の実装やセキュリティに関して検討する必要がある.

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，2019 年 3 月発表予定.