1V-01

QUICにおける仮認証サーバの導入によるハンドオーバの効率化

奥西理貴† 西牧佑哉‡ 佐藤健哉‡

†同志社大学理工学部情報システムデザイン学科
‡同志社大学大学院理工学研究科情報工学専攻

1 はじめに

公衆無線 LAN のセキュリティを確保するため、IEEE802.1X 認証等を用いたユーザ認証が必要不可欠である．このとき，多数設置された公衆無線 LAN での認証を一括管理するために，クラウドサーバ等で遠隔地に認証サーバを設置する運用 [1] が考えられるが，認証サーバへの伝搬遅延が増大するため，ハンドオーバ時の再認証時に遅延が増大する．そのため，特に音声やマルチメディアを扱うアプリケーションでは，サービス中断時間が発生しやすい．

本研究では，この問題を解決するために，HTTP/3 の下位層としても採択され今後の発展が期待される QUIC(Quick UDP Internet Connections) を使用し，ハンドオーバ中の認証処理が完了するより前に一時的に接続を許可することで，認証処理の完了を待たずにアプリケーションフローを再開できるようにする方式を提案する．

2 関連研究

Ioanna らは，IEEE802.11f (IAPP) を用いて，異なるネットワーク間のハンドオーバ遅延を軽減する手法を提案している [2]．しかし，この研究では，IEEE802.1X 認証など RADIUS サーバを用いた認証遅延については考慮されておらず，利用できるのは事前共有鍵方式に限られる．

3 提案手法

3.1 概要

QUIC では，コネクション毎に一意の「コネクション ID (CID)」が割り当てられ，ヘッダに平文で格納される．そこで，アクセスポイント (AP) がこの CID をもとに端末を識別し，認証処理が完了するまでの間，接続を一時的に許可する．この一時的に接続を許可されている状態を本研究では「仮認証」と呼ぶ．

Efficient Wireless LAN Handover with Temporary Authentication Server during QUIC Connection
Riki Okunishi†, Yuya Nishimaki†and Kenya Sato†
†Doshisha University

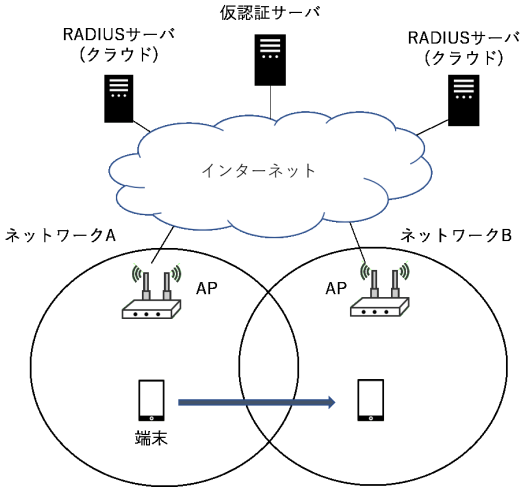

図 1: 提案手法のトポロジ

仮認証を実現するには，端末の利用する CID を移動先の AP と共有しておく必要がある．また，認証処理よりも前にアプリケーションフローを開始するため，無線通信での暗号鍵を用意する必要もある．これらの要件を満たすため，図 1 のようにインターネット上にそれらを配布するためのサーバを配置する．これを「仮認証サーバ」と呼ぶ．仮認証サーバは各 AP と安全な通信路で接続されており，AP からの通知をもとに対象の AP に対して CID と暗号鍵を配布する．

3.2 提案手法の手順

図 2 と図 3 で示すように，提案手法は認証時の動作とハンドオーバ時の動作の 2 段階で構成される．詳細な手順は以下の通りである．なお，図 3 において一部の手順に対応する箇所は省略されている．

1. 端末がネットワークに接続し認証処理を終えると、AP は仮認証サーバに対して接続した端末の情報を通知する．

2. 仮認証サーバが通知を受け取ると，仮認証用の CID と暗号鍵を生成し，端末と端末のハンドオーバ先になりうる候補 AP に対してそれらを配布する．配布される AP は複数台あってもよい．また，仮

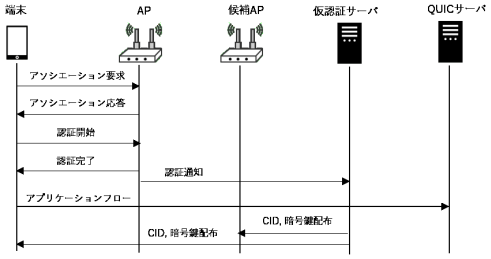

図 2: 認証時のシーケンス図

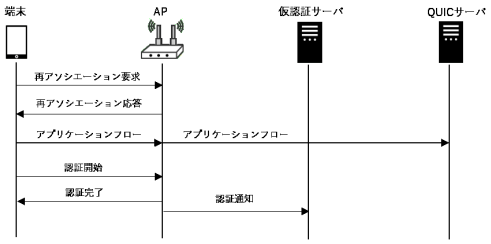

図 3: ハンドオーバ時のシーケンス図

認証サーバは候補 AP を適切に決定できるものとする．

3. 端末がハンドオーバを開始し，移動先の AP とのアソシエーションが完了すると，そのネットワークの認証サーバと認証処理を行いつつ，端末は仮認証を開始しアプリケーションフローを再開する．この時，端末は仮認証サーバから配布された CID を利用し，同時に配布された暗号鍵で暗号化して送信する．

4. AP が仮認証中の端末からパケットを受信すると，対応する暗号鍵で復号し，CID を検証する．一致すればパケットの通過を許可し，一致しなければ失敗を表すフレームを返す．仮認証中の端末からのパケットを初めて検出した時，仮認証サーバに通知を送る．

5. 通知を受けた仮認証サーバは，通知を送信した AP を除いて，ハンドオーバした端末に対応する CID と暗号鍵を配布した他の候補 AP 全てに対し，その情報を削除するよう通知を行う．通知を受けた AP は対応する CID と暗号鍵を削除する．

6. 端末が認証処理を完了すると，端末と AP は CID と暗号鍵を削除して仮認証を終了するとともに，1. と同様の処理を行い次のハンドオーバに備える．

4 評価

評価は，オープンソースの離散事象ネットワークシミュレータ ns-3 を用いて行う．

評価指標として，サービス中断時間を測定する．これは，端末がハンドオーバを開始して AP にアソシエーション要求を送信してから，アプリケーションフローのパケットが初めて通信相手に届くまでの時間とする．アプリケーションフローとしては，140kbps のビデオ会議を再現するために，175 バイトを 10ms ごとに送信するものとする．

認証サーバの認証方式は TTLS を想定し，その処理遅延は参考文献 [3] を元に 30ms とした．同方式を東京—大阪間 (約 400km) で利用した際の伝搬遅延を加味して，認証遅延として 38ms とする．

評価結果を表 1 に示す．

表 1: サービス中断時間

サービス中断時間 (ms)	最小値	平均値	最大値
提案手法なし	60.84	66.58	71.02
提案手法あり	22.35	29.51	39.05

提案手法のサービス中断時間は最大でも約 39ms に抑えられており，参考文献 [4] でも要求されている，50ms 以下の中断時間を満たすことができた．また，最小値，平均値，最大値のいずれも，提案手法ありと提案手法なしとの差は 30ms 以上である．提案手法では認証の完了を待たずにフローを再開できることから，認証遅延と同程度の時間を短縮することができている．

5 おわりに

本研究では，QUIC プロトコルの活用と仮認証サーバの導入によって，ハンドオーバに伴う認証遅延の影響を削減する手法を提案した．シミュレーションによる評価から，伝搬遅延を含む認証遅延を短縮できた．

今後の課題としては，各 AP や仮認証サーバの負荷の状況を考慮して，各 AP の端末の接続台数による影響を検証する必要がある．

参考文献

[1] Cisco Meraki MR シリーズ. https://cisco-start.dis-info.jp/cisco-meraki/mr.html. (Accessed on 01/09/2020).

[2] Ioanna Samprakou, Christos Bouras, and Theodore Karoubalis. Fast and efficient ip handover in ieee 802.11 wireless lans. pp. 249–255, 01 2004.

[3] 厚谷有輝, Souheil Ben Ayed, 寺岡文男. Diameter eap application に基づくネットワークアクセス認証のための eap-ttls の実装. コンピュータソフトウェア, Vol. 29, No. 4, pp. 130–145, 2012.

[4] A. Mishra, Min Ho Shin, N. L. Petroni, T. C. Clancy, and W. A. Arbaugh. Proactive key distribution using neighbor graphs. *IEEE Wireless Communications*, Vol. 11, No. 1, pp. 26–36, Feb 2004.