

オンライン授業資料共有のための携帯端末間認証方式

蘇原 碩威[†] 朝賀 貴裕[†] 清原 良三[†]

神奈川工科大学情報学部情報工学科[†]

1 はじめに

最近大学などの授業で、講義資料が電子化されていることが多く、学生はプロジェクタによる投影画面と手元のノート PC や、タブレット、スマートフォンなどを見ながら受講することが多くなってきた。資料を見るだけでなく、電子的にメモやノートを取ったり、作成した資料を他の学生と共有したりすることも増加してきた。演習も行う授業では、オンラインでプログラムを配布し、実行する場合もあり、必要機材として携帯情報端末を貸し出していることも少なくない。

時間外での予習復習時間を想定したグループワークで情報を共有する場合などで個別に端末間での情報共有が必要となることがある。授業中にそのファイルの転送なども行うことがあるが、必ずしも近い席に座っているとは限らない。

無線機能で接続して簡単に情報を共有できれば良いが、貸与端末を利用していると端末固有の無線機能の ID が授業ごとに毎回変わる可能性が高く、接続先を端末固有 ID のみで判別するのは困難である。また、必ずしもインターネットによる通信が可能であるとは限らず、通信回線が張り巡らされている環境ではない可能性を考慮する必要もある。

そこで、本論文では多くの端末に Wi-Fi や Bluetooth といった無線通信機能が搭載されていることを利用し、サーバを介さず P2P (Peer-to-Peer) による 1 対 1 の無線通信方式で容易に端末を識別、認証できる方式を提案評価し、その有効性を示す。

2 既存技術及び関連研究

通信端末の識別認証する方法として、ジェスチャーや位置推定、画面への入力を用いられている。それらを利用した P2P 通信方式による類似研究は多数行われており、以下の例が挙げられる。

- (1) 加速度センサによるジェスチャー認証[1]

- (2) 電波強度や GPS による位置推定を用いた認証[2]

- (3) NFC を用いた接触型認証[3]

- (4) コード入力による認証[3]

- (5) 指紋や虹彩などの生体認証[4]

- (6) 音声を利用した認証[5]

このように端末間認証方式そのものはいくつも存在するが、いずれも接続先端末が何であるか明確であり、同時に複数の端末へ接続要求を出すことが困難である場合が多い。

また本システムは教室内における利用を想定しているため、音声認証や電波強度といった周辺環境に依存される方式は運用が難しい。

3 利用通信方式の検討

Android 上で利用できる P2P 方式の代表例として Bluetooth 及び Wi-Fi Direct が挙げられる。

表 1 に両者の特性を示す。これにより最大実効速度や通信距離といった点で Wi-Fi Direct の優位性が認められるが、本システムで想定している「教室内での資料共有」という観点から通信距離が 10m でも問題なく、同時に複数の端末へ接続要求を出したいため通信距離が長すぎても冗長である。また、最大実効速度についても端末間認証後送受信するデータの種類としてテキストファイルやといった容量の小さなデータを想定しているため速度は追求していない。よって必ずしも満充電で貸与されるとは限らないことからわざわざでも消費電力の少ない Bluetooth が適切と考えこちらを採用する。

4 提案手法

本論文では、端末固有 ID や端末機種が不明である状態であっても接続先の識別と認証が可能となる方式として、端末ではなく個人が固有識別子を保持する手法を提案し、実装・評価した。

固有識別子として記憶されにくくかつ真似されにくいものとして、画面に入力するスワイプを利用する。

表 1. Bluetooth と Wi-Fi Direct の比較

	Bluetooth	Wi-Fi Direct
通信距離	10m(class 2)	90m
最大速度	1Mbps	250Mbps
消費電力	2.5mW	260mW(2.4GHz)

An Authentication Method between Mobile Devices for Sharing the online Documents

Hirohisa Sohara, Takahiro Asaga, Ryozi Kiyohara
Kanagawa Institute of Technology

表 2. 一致率調査結果

閾値	1.0	1.5	2.0	2.5	3.0	3.5	4.0
実験回数	25	25	25	25	25	25	25
一致数	18	21	20	22	17	14	12
誤一致数	7	4	3	1	0	0	0
不一致数	0	0	2	2	8	11	13
成功率	.720	.840	.800	.880	.680	.560	.480

まず、事前に本人固有のSwipeを貸与端末初回利用時に利用者全員が登録し、データベースとして端末間で共有しておく。

利用時には、発信者は本人固有識別子を入力し周囲へ接続要求を出す。接続要求を受け取った受信者はステータスバーへSwipe登録名が通知され発信者を特定することができる。接続してもよい相手であれば画面へ受信者側が持つ固有Swipeを入力し発信者側と同様に登録されたデータから一致度の判定を行う。一致すると判断されれば発信者へ要求が返送され接続が確立される。

5 基礎実験

認証のための基礎実験として、5人の被験者に対し被験者本人が登録したSwipeをもう一度Swipeした際、自分が登録したものであるかどうかの判定を1つの閾値あたり5度入力し調査した。同時に他の被験者が作成したSwipeと判定される回数も集計した。

また、本システムでは接続要求が通信範囲内すべてへ通知されるため、固有Swipeを真似される可能性がある。

そこで、なりすまし防止のためSwipeを登録した本人以外が入力を真似した場合の誤差を計測するため、1px(Pixel)ごとに座標を抽出し散布図として計測をし、本人入力と比較し誤差の許容範囲算出を行った。

6 結果と考察

基礎実験の結果として、Swipe一致成功率を表2に、非登録者による誤差を図1に示す。

その結果から不一致数及び誤一致数を除いた一致成功率から閾値2.5が適当である。

また、登録者本人が登録したSwipeであれば再度入力しても座標値の誤差はあまり見られなかったが、非登録者によるなりすましSwipeでは座標ごとの誤差が大きいため差別化を図ることができる。よって一致度判定に関する誤差を1座標あたり0.3以内とした。

また、本システムでは接続要求が発信者を中心に放射線状であるため指向性がなく、無関係の端末まで通知が行き届いてしまう。端末間認証確立後に共有したいデータのリクエストを目的とした簡易的なチャットを実装しているが、本

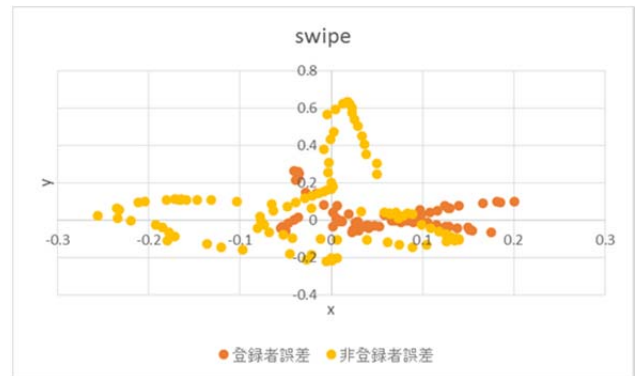


図 1. 誤差比較結果

来の接続先と違った場合もう一度最初から要求を出す必要がある。つまり現状のシステムでは確実な相手との端末間認証に長い時間がかかる。それらの改善が今後の課題である。

7 まとめ

本論文で作成したアプリケーションについて、Bluetoothのピコネット通信方式の特性上、一度に7台までしか接続要求を出すことができないという欠点はどうしてもついて回った。しかしながら、ペアリング後の資料のやりとり自体は1対1で行うものとして開発したため、特に支障はないものと考えた。

さらに、通信可能範囲全体への単一な接続問い合わせではなく、端末の向きなどを感知し特定の端末へ要求を出すなど、指向性の高い機能を実装することで、より直接的な接続要求を出すことが求められる。そうすることで無関係な端末への通知などの負担が減ることが予想され、接続したい端末へ接続要求が通知されないという問題点解消が見込まれ、認証成功率向上も見込めると考えられる。

参考文献

- [1] 稲垣真人, 新城康哉, 福原遼, 狐崎直文, 戸辺義人: 近距離無線通信におけるジェスチャ利用の提案
- [2] 佐藤智美, 小宮山哲, 下田雅彦, 劉渤江, 横田一正: Bluetoothの電波強度を用いた位置推定方式の検討
- [3] <http://ja.wikipedia.org/wiki/Bluetooth>
- [4] 濱野雅史, 新井イスマイル: 加速度センサ・ジャイロセンサを併用したスマートフォンの利用認証手法の提案
- [5] Yasutaka Nishimura, Masaya Yoshida, Kiyohito Yoshihara: A Device Specification Method by Describing a Circle in the Air
- [6] <http://www.silex.jp/blog/wireless/2012/09/blue-tooth1.html>
- [7] <http://www.wdic.org/w/WDIC/Bluetooth>