

近距離通信を用いた親子端末の連携を鍵とするスマートフォン認証

岸里 正樹†

高井昌彰‡

北海道大学大学院情報科学研究科†

北海道大学情報基盤センター‡

1 はじめに

ネットショッピングやアプリのインストールなど、子が単独で操作を行うことが望ましくない状況では、親が子のネット利用を見守り、利用を制限することが必要である。

子の利用する端末にロックをかけ、必要に応じて親が解除を行うという方法では、ロックの解除キーとしてパスコードや画面を指でなぞるパターンを用いた場合、子が親の操作を背後から覗き込むことによって解除キーを容易に盗み取ることが可能である。

本稿では、上記の問題を防ぎ、安全かつ手軽に、親が子を見守りながら認証を行うことを目的として、スマートフォン端末の Bluetooth 機能を利用し、親と子の端末同士を一定距離内に近付けて連携させることで子端末のロックを解除する認証システムについて述べる。

2 システム設計

2.1 認証の流れ

本システムでは、複数の端末を、認証を経て許可の権限を与える親端末と、許可を受ける子端末の2種類に分けて連携させる。認証動作は端末同士の接近を必要とする第一段階及び親端末で操作を行う第二段階に分けられる。

第一段階では、親端末が周辺のデバイスを探索し、子端末を発見したときに距離を取得する。両端末が物理的に一定距離内に接近していない場合、認証の第二段階に進むことはできない。

第一段階の認証を通過した後、予め設定された方法で親端末での第二段階の認証を行う。これを通過することをもって、子端末のロックが解除され、目的の操作を行う権限が与えられる。

また、一度端末同士を近づけて認証が完了し、子端末に権限が与えられた後であっても、端末同士が一定距離以上離れた場合には、再び端末同士の接近と認証動作を要求する。

2.2 第一段階の認証動作

親子端末は Bluetooth による通信を行うため、互いの MAC アドレスを予め登録しておく。

まず、親端末は Bluetooth を用いて近くにあるデバイスをスキャンする。その中から登録した子端末が発見されると、RSSI（電波の受信強度）をもとに端末間の距離測定を開始する。

RSSI 値を s 、距離を r とすると、RSSI から端末間距離の概算値への変換は次式で求めることができる[1]。

$$r = 10^{\frac{(\text{距離 } 1\text{m のときの RSSI} - s)}{(10 * 2.0)}}$$

算出した距離を用いて、親子端末が接近しているかどうかの判定を行う。予め設定した閾値よりも小さければ、端末同士が接近していると見なし、Bluetooth のペアリングを行い、第二段階に移行する。

2.3 第二段階の認証動作

第二段階の認証方法として、パスコードやパターンロック等といった従来の簡易な認証方法を利用すると、第1章で述べたように、子によるショルダーハック等のリスクを回避できない。

そこで、口唇部位の移動による認証システム[2]を用いることとする。このシステムは、図1のように口唇部位を移動させ、スマートフォン端末のカメラで画像認識する。システムは口唇の動きを図2に示すような格子パターン上での方向入力へと変換することで、従来のパターンロック認証と同様の機能を実現するものである。

この認証システムを親端末の認証に用いることによって、パスコードのショルダーハックや、スマートフォン画面上の指の痕跡から認証キーの読み取ることを防止できる。

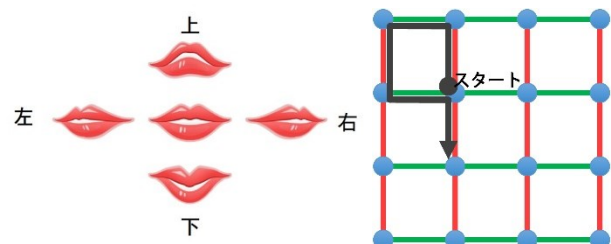


図1 口唇部位の移動

図2 格子状パターンロック

Smartphone user authentication by short-range communication between a parent and a child

†Masaki KISHISATO, Graduate School of Information Science and Technology, Hokkaido University

‡Yoshiaki TAKAI, Information Initiative Center, Hokkaido University

2.4 一対多及び多対多での利用

親端末と子端末を連携させる際、必ずしも一対一の対応に限定されるものではない。例えば、1台の親端末が複数台の子端末に対して同時に権限を与える場合や、複数台の親端末が全て許可しなければ子に権限を与えないようにする場合、あるいは、複数の親端末のうち1台でも許可すれば子に権限が与えられる場合など、多様な連携が想定される。

図3に親と子が一対一の関係にある場合の構成を示す。親端末と子端末が複数台であっても、接近待ちから認証動作及び認証待ちへの状態遷移における条件並びにロック解除に必要な条件が複数台に対するものになるのみである。

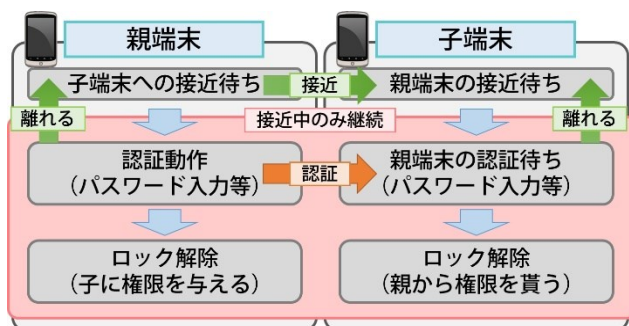


図3 システムの構成図

2.5 実装環境

認証システムを動作させるスマートフォンには、親端末として au LGL21(OS : Android 4.0.4, CPU : 1.5GHz(4C)), 子端末として Docomo SC-02E(OS : Android 4.3, CPU : 1.6GHz)を用い、本システムの開発言語には Java を用いた。

3 実行結果

親端末1台と子端末1台を連携させ、認証動作を行った際の動作画面の例を図4に示す（ロック解除後に子端末が利用可能となる機能として Amazon でのネットショッピングを想定）。

実験において、2台の端末を共に移動させていないにもかかわらず、更新を行うたびに RSSI 値が大きく変動してしまうことがあった。その結果、端末同士が近いにもかかわらず、親端末が子端末を発見できず接続できないことがあった。一方、端末同士が離れている場合に近いと誤認識されることはなかった。現在の実装では、子端末を発見できない場合に、親端末が Bluetooth の発見待ちをリセットする。

また、Bluetooth のペアリングを行っている際

に RSSI の取得が行えない状況も見られた。この場合も、ペアリングのリセットを行うことで再び取得できるようになるが、値の更新が遅れ、認証動作のリアルタイム性が失われてしまう問題点がある。安定して RSSI 値を取得できる実装方法を検討する必要がある。

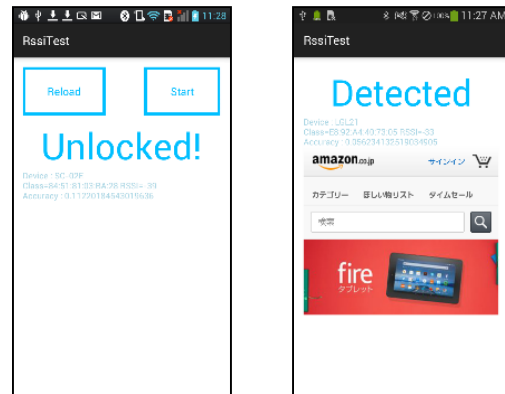


図4 親子端末の動作画面（端末検出とロック解除）

4 まとめと今後の課題

本稿では、スマートフォン端末同士を一定距離内に近付けることでロックの解除を行うことのできる認証システムについて述べた。

第2章では親子端末によって行う認証にのみ重点を置いた実装方法について述べたが、認証の完了後も親が継続して子のネット利用を見守ることのできる機能の実現を検討している。子端末に対しブラウジングを許可した際には、ブラウザのスクリーンショットを親端末に定期的にサンプリングして親端末に送信し、また、アプリのインストールを許可した際には、そのアプリの詳細な情報を親端末に送信するといった機能が例として考えられる。

その他、なりすまし防止のための暗号化の実装、RSSI 取得方法の改善、他 OS への移植が今後の課題である。

参考文献

- [1] Erin-Ee-Lin Lau, Boon-Giin Lee, Seung-Chul Lee, Wan-Young Chung: "Enhanced RSSI-Based High Accuracy Real-time User Location Tracking System for Indoor and Outdoor Environments", (<http://www.s2is.org/Issues/v1/n2/papers/paper14.pdf>, 参照: 2015/12/28)
- [2] 岸里正樹, 高井昌彰: 井口唇領域の動きの画像認識を用いたスマートデバイス向けパターンロックシステム”, 第14回情報科学技術フォーラム (FIT2015), M-031, Vol.4, pp.363-364 (2015)