講演番号：53

BLE Beacon を用いた公衆無線 LAN における相互認証方式

B－7　Mutual Authentication Method in Public Wireless LAN using BLE Beacon

坂井　俊介†　手塚　広太†　新津　善弘†

Shunsuke SAKAI†　Kota TEDUKA†　Yoshihiro NIITSU†

† 芝浦工業大学システム理工学部電子情報システム学科

† College of Systems Engineering and Science, Shibaura Institute of Technology

1.　まえがき

近年，訪日外国人観光客への通信環境整備の需要に対し，公衆無線 LAN の設置数が増加している一方で，認証等のセキュリティ面に問題があり，セキュリティの確保は急務である．

2.　従来方式と問題点

従来研究[1]では，公衆無線 LAN の相互認証を行う方式として，NFC（Near Field Communication）を用いた方式を提案している．しかし，NFC の特性上，ユーザが認証発行機まで接近する必要があり，複数のユーザによる利用の際に待ち行列が発生しやすく，利用開始までの利便性が低い．

2.1.　従来方式

NFC による通信を用いて，利用者端末と認証サーバ間で相互認証に必要なデータのやり取りを行う．システムの概要を以下の図 1 に示す．

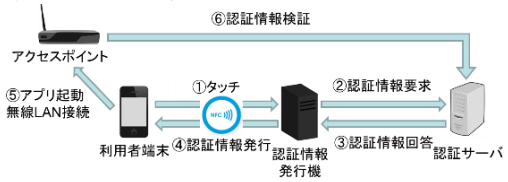

図 1．従来方式のシステム概要

3.　研究概要

3.1.　目的とアプローチ

駅構内での公衆無線 LAN の短時間利用における利便性向上を目的に，BLE Beacon の電波を受信した端末が自動で認証を実施する相互認証方式を提案し，評価する．

3.2.　想定環境

本稿では，公衆無線 LAN の利用者は認証発行用のアプリケーションを自身の端末にインストールしており，利用者端末は認証サーバや公開鍵サーバとモバイル回線等での通信が可能であるものとする．また，公衆無線 LAN の SSID とパスワードはシステム管理者が任意に変更することが可能である．

3.3.　各機器の名称と役割

- BLE Beacon

本システムに対応した BLE Beacon として，事前に設定したアクセスポイントごとの UUID，公開鍵情報と対応した Public Search，一定時間ごとに更新されるワンタイムパスワードを一定間隔で発信する．

- 利用者端末

認証発行用のアプリケーションがインストールされている．

- 公開鍵サーバ

ワンタイムパスワードを用いたワンタイム認証と公開鍵の管理を行う

- 認証サーバ

ユーザ情報と認証情報による相互認証とアクセスポイント情報の管理を行う．

- アクセスポイント

システム管理者が任意で設定したパスワードによるセキュリティを有した，公衆無線 LAN のアクセスポイント

4.　提案方式

システムは，ワンタイム認証と相互認証の 2 つのフェーズに分かれており，BLE(Bluetooth Low Energy) Beacon の電波を受信した端末が自動で認証を実施する．システムの概要を以下の図 2 に示す．

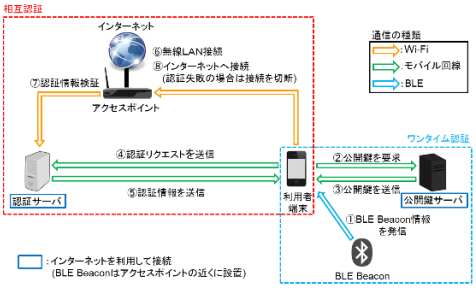

図 2．提案方式のシステム概要

5.　評価

5.1.　評価項目

- 認証時間[ms]
- 単位時間あたりの認証発行数[回/分]
- 通信量[kB]

5.2.　実験結果

評価実験によって得た結果を図 3，図 4 に示す．また，提案方式における通信量は 3.13kB であった．

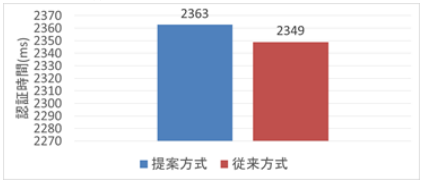

図 2．認証時間

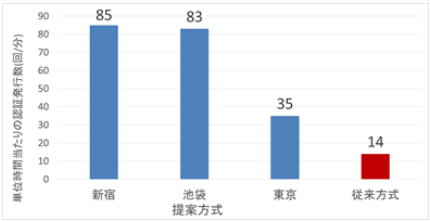

図 3．単位時間あたりの認証発行数

6.　考察

図 3 より認証時間は従来方式の方が提案方式よりも優位であるが，その差である 15ms と，提案方式における通信量は大きくないといえる．また，図 4 より単位時間あたりの認証発行数が 14 回を超える環境においては，提案方式の方が優位であると考えられる．

7.　むすび

本稿では，BLE Beacon を用いた相互認証方式を提案し，評価実験を行った．今後は，実環境に近い実験を実施し，提案方式の有効性を示すとともに，認証時間とモバイル回線使用時の通信量の削減を目指す．

参考文献

[1]宮下悠生，橋本周平，福井千晶，藤村真生 “NFC を用いた公衆無線 LAN 接続環境の構築”，FIT2016，L-023 (2016)