M-022

Smart Building の機器操作における、Location-Proof 機構を使用したアクセス制御の実現
Access-control using Location-Proof mechanism in Smart Building environment

佐々木 美穂　　越塚 登
Miho Sasaki　Noboru Koshizuka

1. 研究背景

ビル設備をネットワークを介して管理・制御できる、Smart Building の開発が進められている。Smart Building では空調や照明、スマートメータや各種環境センサ、エレベータなどに RESTful な API が整備されているが、ユーザがこれらを管理・制御するには、ビル内に設置されている同様の機器の中から対象となる機器を適切に選択し制御する必要がある。またユーザの属性に応じて制御できる機器は適切に制限されなければならない。例えばユーザの部屋に設置された冷暖房装置の制御は許諾されるべきで、他の部屋の冷暖房装置にはアクセスできないよう制限されるべきである。

2. 研究概要

Smart Buildingにおいての機器操作は通常サーバー上にAPIリクエストを送ることで行われていることが多い。また多くのビルではユーザごとにアクセスできる機器を制限しなければならないケースがある。例えばビル来訪者などは操作可能な機器を最小限に機器のみ操作を制限したい。その場合、ユーザごとのアクセス制御はサーバー上にデータベースをもち、APIのリクエストに対してユーザ認証を行うことで、ユーザごとにアクセスできる機器へのAPIを制御している。

現状のSmart Buildingではユーザごとの機器操作の制御は行うことができるが、ユーザが現在いる位置によって制御を変えることはできない。例えばその部屋にユーザがいなくとも、機器を操作することは可能である。ビルによっては部屋などにより管理者が異なることもあり、全く別の部屋の権限まで与えてしまうことは権限管理としてはよくない。一時的にその部屋にいる人に操作権限を与えたい場合などは、手動で権限を与えなければならない。そこで、ユーザの現在いる位置情報を利用することで、機器操作の制限を実現することが本研究の主な目的である。

携帯端末などの位置情報を使用した屋内におけるシステムの研究は多数行われている。例えば携帯端末の位置情報を使用し、携帯端末の位置から目的地まで誘導するナビゲーションシステムが開発されている。しかしながら、多くの研究では携帯端末で得られた位置情報をサーバー側に直接送っているため、デバイス側でデータを詐称された場合に、ユーザが位置を詐称できてしまう可能性がある[1]。

Smart Buildingの機器制御の際に位置情報を利用するには、まず位置情報が詐称されないことへの保証が必要である。ユーザがその部屋にいなくとも、位置情報を変えてしまうことが可能であれば適切に機器制御できているとはいえない。

また、署名を使用した手法も行われているが、署名の秘密鍵の管理をデバイスで行っており、また近くにあるデバイスで署名を行っているという点からSmart Buildingのシステムで運用する際に、鍵の管理の問題が発生する［2］。

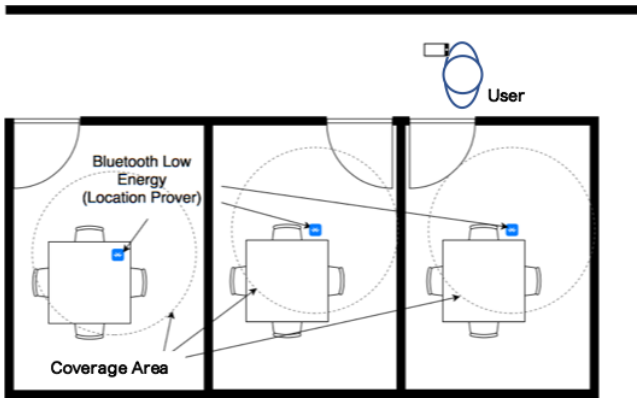

図 1　配置図

本研究で実装するシステムの目標は位置をユーザが詐称できないようにし、適切な機器制御が行われることである

また適切な機器制御を行う際に、位置情報をどのように使用するのかという点も考慮しなければならない。例えば、Smart Buildingの機器操作などは部屋ごとで行われることが多く、ユーザがどの部屋にいるのかという情報が必要な場合が多い。そのような場合、部屋の大きさ・建物のレイアウトなどは建物によって異なるが、建物・部屋の情報にかかわらず位置情報からユーザの正しい位置を把握したい。

想定されるユーザ体験としては、ユーザが携帯端末のアプリケーションを介してユーザの近隣もしくは部屋にある機器のみ操作を行うことができ、またユーザ自身が自分の位置を詐称できなくすることが期待できる。

3. 認証システムの概要

今回の研究では、まずユーザに位置情報を詐称されないようにすることが必要である。そのため位置情報をサーバー側でなく、近くに設置した Bluetooth 通信が可能な機器(Location Prover)で受け取り、そこで暗号化したものをサーバーに送ることで詐称を防ぐ。具体的な設置場所を図 1 に示す。図 1 のように、部屋ごとに機器を設置し、Bluetooth の電波が受信できる位置にユーザがいなければ機器を操作できない。今後この機器のことを Prover と呼ぶ。

今回Proverを選択した理由としては、位置情報を用いたサービスの場合、ビーコン側から位置情報を発信するのみであり、その場合受け取ったデバイス側で位置情報を書き換えられる可能性がある。それを防ぐためには、デバイス側からビーコン側に接続し、そのデータを暗号化した上でデバイス側に渡すことが一つの方法として挙げられる。赤

外線・可視光線など、その他様々な方法でのアプローチも存在しているが、今回は最終的に機器操作を行うアプリケーションとして実現することから、Bluetooth通信を用いた方法を採用した。

全体のアーキテクチャを図２に示す。具体的な構成について、携帯端末のアプリケーション側で行っている部分・Location Prover・サーバーでおこなっている認証部分に分けて説明する。

4.1 アプリケーション側

Smart Buildingにおける機器操作として、携帯端末のアプリケーションを使用することを想定している。また、アプリケーションを開くと、ユーザが制御できる機器一覧が表示される。

アプリケーションから機器へ接続する操作として、まず近くにある Location Prover への接続を要求する。近くに Location Prover が見つかった場合、Prover に接続し、認証に必要な token を受け取る。その token を使用することで最終的に Smart Building の機器操作の API を実行することが可能になる。

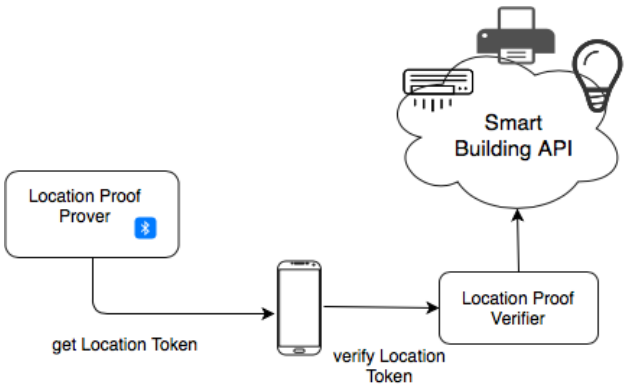

図２　システム概要

4.2 認証側

Proverは各部屋に設置し、各Proverの電波が到達する範囲内のみで機器の操作が可能となるが、部屋の大きさによっては電波の強度を調整することが必要になる。Proverは Bluetooth同士で使用可能である、Generic Attributes(GATT)とよばれる階層データ構造を使用する。GATTを使用することで携帯端末とProverとの間でデータのやりとりが可能になる。またGATT内には複数のCharacteristicと呼ばれる値を保持できる機構がある。このCharacteristicでは規格で定められており、データの書き込み・読み取り・通知・ブロードキャストなどが可能になる。本研究の実装では、Proverは常にBluetooth peripheralの読み取り可能なCharacteristicを発信しており、携帯端末からの読み取り要求があった場合に、接続した端末のmac addressおよびtimestampを秘密鍵で署名し、端末へ送信する。秘密鍵・公開鍵のペアはサーバー側とProver側でそれぞれ管理している。

以上の構成によりどのデバイスから・どの時刻に接続があったのか、情報を記録することができる。

4. 実装

今後の具体的な実装方法に関して述べる。

現段階では、raspberry pi2 台・Android 端末を使用し、隣接した 2 部屋にそれぞれ 1 台ずつ設置し、Android 端末上のアプリケーションにおいて、端末が部屋にある際に、部屋の Location Prover に接続し、データを受け取れることを確認した。今後の実装では、端末側から受け取ったデータをサーバー上で検証する。今回これを Location Proof Verifier と呼ぶ。Verifier の方で検証し、実際に Smart Building の機器操作に位置情報を組み込み、動作検証を行う。

5. 今後の課題

今後の課題としては以下のものが挙げられる。

まず、この研究においてProverがそれぞれ秘密鍵をもっておくことが前提になるが、Proverは直接Smart Buildingのサーバーにアクセスしていないために、鍵の交換方法を検討する必要がある。Proverは直接Smart Buildingのサーバーにつながってはいないので、方法を考える必要がある。

また最終的に Smart Building で運用する際に、ユーザ情報との紐づけ・アクセスコントロールの問題がある。Smart Building において、誰が建物のどの部分まで入室してよいのかといったアクセスコントロールがあり、ユーザ情報に基づいて管理されている。そのユーザ情報とどのように組み合わせていくのかといった部分を検証することが今後の課題である。

参考文献

[1] F. Campana, A. Pinargote, “Towards an indoor navigation system using Bluetooth Low Energy Beacons”, *2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM)*, Salinas, 2017, pp. 1-6.

[2] Marcos Portonoi, Chien-Chung Shen, “Loc-Auth: Location-Enabled Authentication through Attribute-Based Encryption”, 2015 International Conference on Cpmputiong, Networking and Communications, Communications and Information Security Symposium, pp.89-93 (2015).

[3] Zhichao Zhu, Guohong Cao, “APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services”, IEEE INFOCOM, 2011, pp1889-1897 (2008).