

## Bluetooth の ad-hoc ネットワークを用いた 出席管理システムの構築

庄司悠人<sup>†</sup> 武田敦志<sup>†</sup>

現在、大学講義の出席確認に用いられるシステムは点呼や出席カードの配布、顔認証、指紋認証、BLE ビーコン、GPS を用いたものなどが存在する。これらの既存システムには、導入コストの削減や学生が講義室にいることを証明する範囲の精度向上といった課題が存在する。そこで本論文では、専用の機器を用いないことで導入コストを低くし、Bluetooth を用いることで、学生が講義室にいることを証明する範囲をより限定し、屋外でも利用可能なシステムを提案した。シミュレーションと実機検証により、提案するシステムを用いて出席確認が可能なことを確認した。

### Attendance Management System on Bluetooth Ad-Hoc Network

Yuto Shoji<sup>†</sup> and Atsushi Takeda<sup>†</sup>

Attendance management systems are required in almost all universities. Therefore, many attendance management systems, which uses face recognition, finger print, BLE beacon or GPS, have been developed in order to check attendees in a classroom. The existing systems, however, have problems with cost or accuracy. In this paper, we propose a new attendance management system which uses bluetooth ad-hoc networks. In the proposed system, all smart phones communicate with each other using bluetooth and check other attendees in the classroom. The data of attendees are aggregated via a bluetooth ad-hoc network, and teachers get a list of attendees. This system is constructed by only smart phones which can communicate using bluetooth, so any other special devices are not required. In addition, Range of bluetooth communication is limited, so the proposed system creates a list of attendees accurately. In this paper, we show experiment results which indicates performances of the proposed system.

### 1. はじめに

現在、大学講義の出席確認のシステムとして、点呼や出席カードの配布、顔認証、指紋認証、BLE ビーコン、GPS を用いたものなどが存在する。東北学院大学においても礼拝出席を管理するシステムには学生証を専用の機器で読み取ることで出席とする仕組みが用いられている。これらの既存システムには、導入コストの削減や学生が講義室にいることを証明する範囲の精度向上といった課題が存在する。

導入コストを削減できるシステムとして、講義室内に設置されている Wi-Fi のアクセスポイントを用いるシステムが存在する[1,2,3]。このシステムでは、Wi-Fi のアクセスポイントを用いることで、導入コストが削減できる。しかし、Wi-Fi が講義室の外まで届いてしまう可能性がある。一方、BLE ビーコンなどの専用の機器を用いたシステムでは講義室内にいることを証明する範囲は専用の機器によって、限定できる[4]。しかし、専用の機器が必要になることから導入コストが増加してしまう。他にはスマートフォンの GPS を利用したシステムが存在する[5]。このシステムでは、屋内では精度が低下するといった問題がある。

そこで本論文では、スマートフォンに搭載されている Bluetooth 機能を利用し、講師と複数の学生がアドホックネットワークを構築することで出席確認が可能なシステムを提案する。Bluetooth は Wi-Fi に比べて電波の届く範囲が狭いため、講義室の外にいる学生が出席となることを防ぐことができる。また、BLE ビーコンのような専用の機器を用いないので導入コストの削減ができる。そして、アクセスポイントのような特定の場所に縛られずに使用できるので屋外でも利用可能である。学生の出席を認証する判断基準として、講師のいるアドホックネットワークに接続していること、そのアドホックネットワーク内で講師が複数の学生と直接接続していることを条件としている。そうすることで、出席には講師が複数の学生の認証が必要となり、不正行為を防ぐことができる。評価と検証として、提案するシステムの性能を示すために、シミュレーションと実機検証を行った。シミュレーションでは人口密度と認証成功率、人口密度と最大ホップ数の関係をグラフに示す。また、認証に必要な受信数の違いによる認証成功率と最大ホップ数の変化を示す。実機検証ではスマートフォンの代わりに Raspberrypi3 を使用した。検証の結果として、900 m<sup>2</sup>の講義室で提案システムを利用した場合、約 26 秒かかることが分かった。この数値は出席確認にかかる時間として、講義の妨げにはならないと考えられ、提案システムを用いて出席確認をすることが可能であることを確認した。

本論文の構成は、次のとおりである。2 章では提案するシステムと関連研究との比較を行う。3 章では提案するシステムの事前準備及びシステムの流れ、セキュリティ

<sup>†</sup> 東北学院大学教養学部  
Faculty of Liberal Arts, Tohoku Gakuin University

について述べる。4章ではシミュレーションと実機検証から提案するシステムの性能を示す。

## 2. 関連研究

各講義室に設置されている Wi-Fi のアクセスポイントを利用し、学生が講義室内に居ることを証明する出席管理システムが提案されている[1,2,3]。既に設置されているアクセスポイントを用いるので専用の機器を必要とせず、導入コストの削減ができる。一方、問題点として Wi-Fi の電波の届く範囲の広さが挙げられる。具体的には講義室内に設置されているアクセスポイントに講義室の外から学生が接続できてしまう場合が考えられる。実際に、宮城教育大学の無線 LAN アクセスポイントを用いる出席管理システムでは、建物や階数の異なるアクセスポイントに接続してしまう問題が生じた[3]。

それとは反対に、学生が講義室に居ることを証明する範囲を限定できるシステムとして、専用の機器を用いたシステムが提案されている[4]。このシステムでは専用の機器に数センチから数メートルほど近寄る必要があるため、講義室の外に居る学生が出席となることはない。専用の機器は、BLE ビーコンや IC カードリーダー、顔認証するためのカメラなどが挙げられる。一方、問題点として専用の機器が必要なことから導入コストが高くなることが挙げられる。

他には、屋外でも使用できるシステムとして、スマートフォンの GPS を利用したシステムが提案されている[5]。このシステムでは携帯端末に備わっている GPS を用いて、学生が講義室内に居ることを証明する。スマートフォンに予め備わっている GPS 機能を用いるため、専用の機器を必要とせず、導入コストの削減ができる。一方、問題点として屋内での使用はマルチパスによる乱反射で正常な電波受信が困難であるため、大幅に精度が低下することや階数の特定が難しいことが挙げられる。

本論文で提案するシステムでは、Bluetooth は電波の届く範囲が狭いため、Wi-Fi や GPS と比べて、学生が講義室内に居ることを証明する範囲を限定することが可能になり、屋外でも使用できる。また、専用の機器を必要としないため、導入コストは低くなる。

## 3. ad-hoc ネットワークを用いた出席管理システム

### 3.1 提案システムの概要

提案するシステムでは、Bluetooth のアドホックネットワークを構築し、そのアドホックネットワーク内に居ることを講義室内に居ることを証明とする。MAC アドレスを用いて学生を特定し、代返(なりすまし)を防ぐ。各学生のデジタル署名によって、内容の改ざんを防ぐ。出席確認を講義中にランダムに数回行うことで途中退室を防ぐ。

デバイスはスマートフォンを用いる。前提として MAC アドレスは偽装不可とする。学生の出席を認証する判断基準として、講師のいるアドホックネットワークに接続していること、そのアドホックネットワーク内で講師が複数の学生と直接接続していることを条件としている。そうすることで、出席には講師が複数の学生の認証が必要となり、不正行為を防ぐことができる。

提案するシステムでは、講義室が広がるほど学生を認証するためには最大ホップ数が増える。その最大ホップ数も人口密度によって変化すると考えられる。理由を図1に示す。左図のように端の学生と講師の間に中継する学生がいない場合、回り込むような形で中継していくため、最大ホップ数が増加する。反対に、人口密度が高いと講師と端の学生の間に中継する学生がいるので、最大ホップ数は減少し、一定の数値に収束すると考えられる。

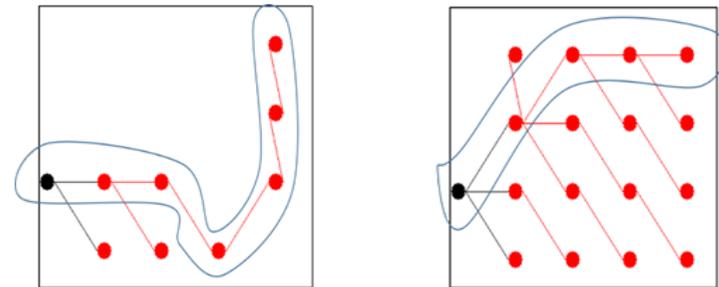


図1 人口密度による最大ホップ数の違い

### 3.2 出席をとる前に行う事前準備

出席をとる前に行う事前準備として、学生はアプリケーションと講師の公開鍵を端末にダウンロード、学生の端末で学生用の秘密鍵を生成、学生の公開鍵、学生番号、MAC アドレスをサーバに登録する。講師はアプリケーションと講師用の秘密鍵を端末にダウンロードする。なお、講師の秘密鍵は、講師一人ひとりを区別する必要はないので、複数の講師が1つの秘密鍵を共有する。故に、学生がダウンロードする公開鍵も一つのみとなる。

### 3.3 提案するシステムの流れ

提案するシステムの流れを図2に示す。まず初めに、図2の(1)のように全ての学生は未認証とする。次に、図2の(2)のように講師が近くにいる学生に送信していく。講師から受信した学生は、認証済みとなる。講師から送られてくる内容は、日付や講義名、担当者名などの文字列と講師のMAC アドレス、講師の秘密鍵で作成されたデジタル署名の3つである。デジタル署名を学生が講師の公開鍵で復号し、講師のMAC アドレスが改ざんされていないかを確認する。そして、確認した講師のMAC アドレ

スと接続しているMACアドレスが同じだった場合、講師の近くにいる学生は講師と接続したと判断できる。図2の(3)のように認証済みのn人の学生から受信した学生は認証済みとなる。デジタル署名は講師のみが作成ができる。したがって、学生はデジタル署名が改ざんされていないのならば、講師がいるネットワークだと判断することができる。周辺に未認証の学生がいない場合、一定時間を過ぎると、講師側の学生に返送する。順次、図2の(4)のように端末側から受信した情報と自分の情報を講師側の端末へ返送していく。この時、学生が返送する内容は、日付や講義名、担当者名などの文字列、自分と通信相手の学生のMACアドレス、学生の秘密鍵で作成したデジタル署名の3つである。講師は学生から出席を集めた後、サーバに送信する。サーバに送信後、学生の公開鍵とデジタル署名を用いて、改ざんやなりすましの有無を調べる。

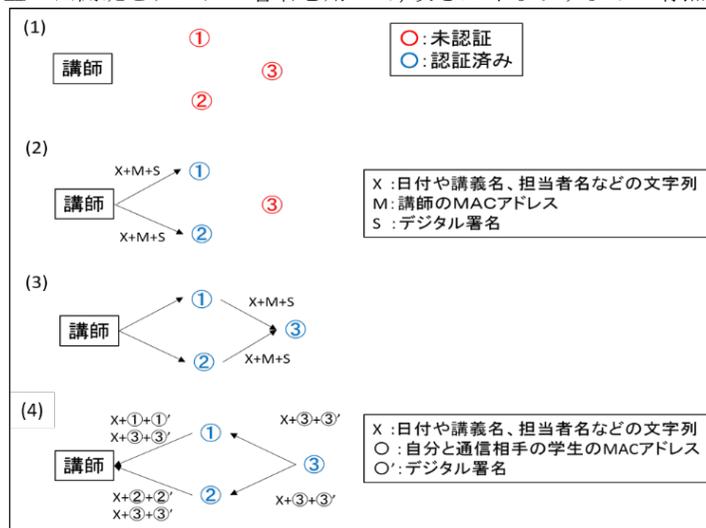


図2 システムの流れ

### 3.4 提案システムのセキュリティについて

提案システムのセキュリティについて述べる。内容の改ざんは各学生のデジタル署名によって防ぐことができる。学生のなりすましはMACアドレスによって防ぐことができる。盗聴は、通信内容はMACアドレスとデジタル署名なので、対策はしない。通信内容の破棄は講師へ続くルート全てに流すことで、対応する。講師がいるネットワークかどうかは講師のデジタル署名によって判断できる。講師と接続したかどうかは講師のMACアドレスをデジタル署名で暗号化することで判断できる。この方法では学生が講師のMACアドレスを事前に知らなくとも問題はない。複数の学生から受信するメリットは一人の学生が他人の秘密鍵を用いて、存在しない学生のデータを作

成し、代返することを防ぐことや講師へ情報を送る際にルートが複数存在する場合、破棄されても他のルートで送ることが可能となることが挙げられる。自分以外のMACアドレスを送信するメリットは通信相手の学生のMACアドレスを送信することで、講師は経路情報を集めることができ、誰が誰を認証したかを判別できることが挙げられる。

## 4. 評価と検証

### 4.1 シミュレーション

人口密度と認証成功率、人口密度と最大ホップ数の関係をグラフに示す。また、認証に必要な受信数の違いによる認証成功率と最大ホップ数の変化を示す。講義室の大きさは、100 m<sup>2</sup>、225 m<sup>2</sup>、400 m<sup>2</sup>、900 m<sup>2</sup>の4つとし、認証に必要な受信数は1~4つとした。OSはWindows10、言語はJavaを用いて実装した。人口密度のサンプルの間隔は10人、電波範囲約10m、各人口密度でシミュレーションを100回繰り返す、平均値を算出した。学生の座席はランダムに振り分けられ、学生は1 m<sup>2</sup>に最大2人が座れるものとする。縦軸がそれぞれ認証成功率と最大ホップ数、横軸が人口密度、認証に必要な受信数は、青色が1、茶色が2、灰色が3、黄色が4となっている。

### 4.2 認証成功率

図3に縦が10m、横が10mの100 m<sup>2</sup>の講義室の認証成功率のシミュレーション結果を示す。100 m<sup>2</sup>の講義室では20~30人を想定している。図3では、人口密度のサンプル間隔は10人なので、人口密度は0.1[人/m<sup>2</sup>]が最小となる。その最小の0.1[人/m<sup>2</sup>]から認証成功率は100%になっている。つまり、100 m<sup>2</sup>の講義室では学生が10人以上いた場合に認証成功率は100%になることが分かる。また、全ての線が重なっていることから認証に必要な受信数の違いによる認証成功率の変化はないことが分かる。図4に縦が15m、横が15mの225 m<sup>2</sup>の講義室の認証成功率のシミュレーション結果を示す。225 m<sup>2</sup>の講義室では40~70人を想定している。図4では、人口密度が約0.09[人/m<sup>2</sup>]以上ならば認証成功率が100%になっている。つまり、225 m<sup>2</sup>の講義室では学生が21人以上いた場合に認証成功率は100%になることが分かる。また、認証に必要な受信数が3つの灰色と4つの黄色が認証成功率に変化が生じている。人口密度が約0.05[人/m<sup>2</sup>]の認証成功率は、青色と茶色は100%になっているのに対して、灰色は95%、黄色は85%となっている。図5に縦が20m、横が20mの400 m<sup>2</sup>の講義室の認証成功率のシミュレーション結果を示す。400 m<sup>2</sup>の講義室では80~120人を想定している。図5では、人口密度が0.075[人/m<sup>2</sup>]以上ならば認証成功率が100%になっている。つまり、学生が30人以上いた場合に認証成功率が100%になることが分かる。また、認証に必要な受信数の違いにより、青色が最も少ない人数で認証成功率が100%となり、続いて茶色、灰色、最後に黄色の順となっている。図6に縦が30m、横が30mの900 m<sup>2</sup>の

講義室の認証成功率のシミュレーション結果を示す。900 m<sup>2</sup>の講義室では100~200人を想定している。図6では、人口密度が0.78[人/m<sup>2</sup>]以上ならば認証成功率が100%になっている。つまり、学生が71人以上いた場合に100%になることが分かる。また、認証に必要な受信数の違いにより、図5と同じく、100%になるために必要な人数の少ない順で並べると、青色、茶色、灰色、黄色の順番になっている。

以上の結果から認証に必要な受信数が多いほど、認証成功率を100%にするためにはより多くの人が必要になることが分かる。また、提案システムでは非常に少ない人数の場合、具体的には100 m<sup>2</sup>であれば10人未満、225 m<sup>2</sup>であれば21人未満、400 m<sup>2</sup>であれば30人未満、900 m<sup>2</sup>であれば71人未満しか学生がいない場合には認証成功率は100%にならず、提案システムが有効であるとは言えない。その対策としては、シミュレーションではランダムに配置していた学生を実際の講義では予め前の席に座らせる、講師が抗議室内を歩き回って認証していくなどの工夫が必要となる。

### 4.3 最大ホップ数

図7では100 m<sup>2</sup>の講義室の最大ホップ数のシミュレーション結果を示す。最大ホップ数は人口密度に比例して増加していく。そして、1ホップに収束する。つまり、中継する学生が一人いれば全ての学生を認証できると言える。認証に必要な受信数の違いによる変化は見られない。図8では225 m<sup>2</sup>の講義室の最大ホップ数のシミュレーション結果を示す。人口密度の増加に応じて最大ホップ数は減少し、1ホップに収束している。また、認証に必要な受信数の違いにより、最大ホップ数が変化している。黄色が一番多く、次に灰色、そして茶色、最後に青色の順となっている。図9では400 m<sup>2</sup>の講義室の最大ホップ数のシミュレーション結果を示す。初めは最大ホップ数が増加していくが、人口密度が0.75[人/m<sup>2</sup>]を過ぎたところから減少していき、2ホップに収束していく。図10では900 m<sup>2</sup>の講義室の最大ホップ数のシミュレーション結果を示す。初めは最大ホップ数が増加していくが、人口密度が0.6[人/m<sup>2</sup>]を過ぎたところで減少していき、3ホップに収束していく。

以上の結果を踏まえると、最大ホップ数の多い順は黄色、灰色、茶色、青色の認証に必要な受信数が多い順になっていることから、認証に必要な受信数が多いほど、最大ホップ数が増加することが分かる。そして、人口密度が増加すると、一定の最大ホップ数に収束していることが分かる。このことから図1で述べた通り、人口密度が低いと最大ホップ数は増加し、反対に、人口密度が高いと最大ホップ数は減少することが分かった。しかし、図9と図10に示す通り、初めは最大ホップ数が少なく、人口密度の増加に応じて最大ホップ数が増えている場合もある。これは認証成功率が関係している。図5と図6に示す通り、図9と図10の人口密度の増加に伴って最大ホップ数が増加している場合は認証成功率が100%に達していない。つまり認証されていない学生が存在するということである。したがって、講師から離れている学生などは認証されないので最大ホップ数は少なくなる。

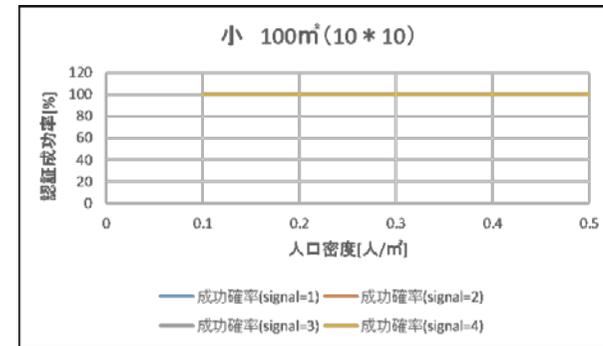


図3 100 m<sup>2</sup>の認証成功率

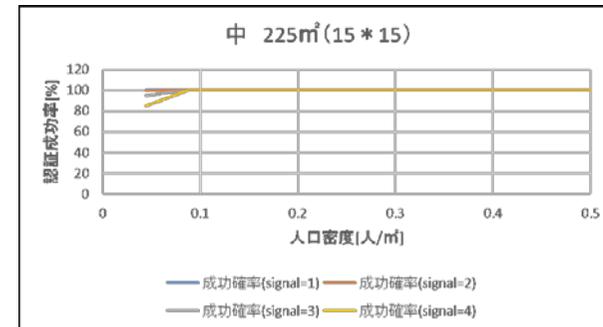


図4 225 m<sup>2</sup>の認証成功率

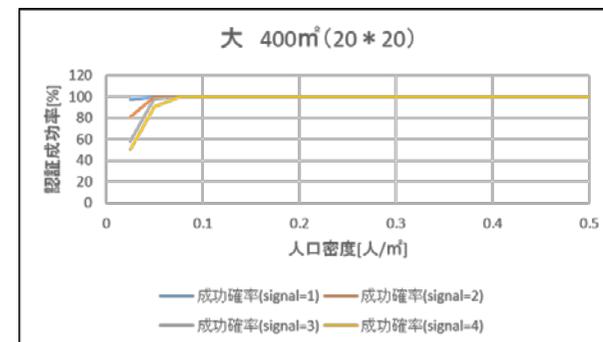


図5 400 m<sup>2</sup>の認証成功率

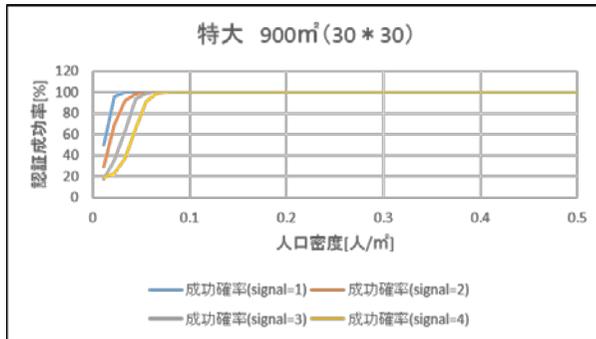


図 6 900 m<sup>2</sup>の認証成功率

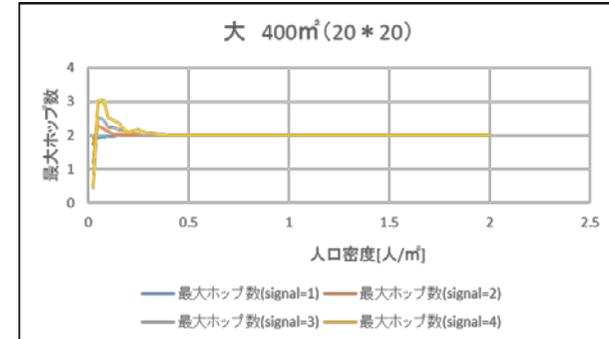


図 9 400 m<sup>2</sup>の最大ホップ数

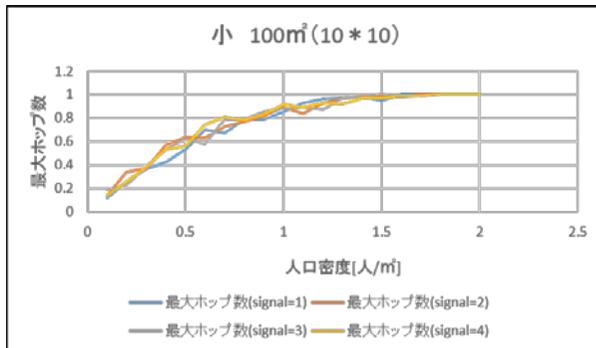


図 7 100 m<sup>2</sup>の最大ホップ数

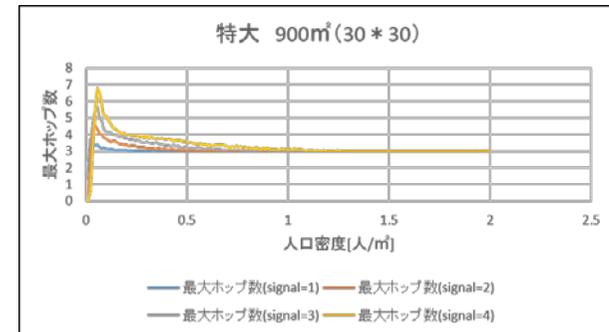


図 10 900 m<sup>2</sup>の最大ホップ数

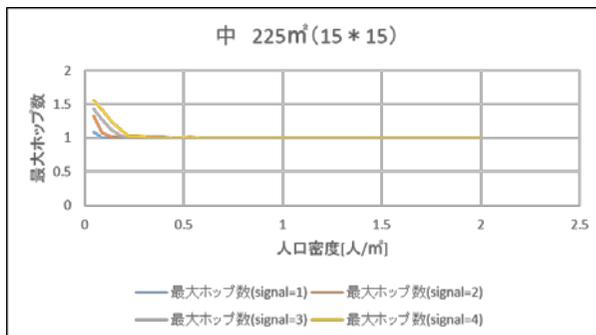


図 8 225 m<sup>2</sup>の最大ホップ数

#### 4.4 実機検証

スマートフォンの代わりに 4 台の Raspberry3 を用いて検証を行った。OS は RASPBIAN, 言語は Javascript, ライブラリは noble と bleno を用いて実装した。ここで Raspberry3 には Bluetooth アダプタを追加している。元々、内蔵している Bluetooth アダプタと合わせて、計二つのアダプタを一台に持たせた。これは noble と bleno を同時に使用するには、二つの Bluetooth アダプタが必要になるためである。なお、これはライブラリの問題であるため、スマートフォンの場合は、ライブラリが異なるので、このような問題はなく、Bluetooth アダプタを追加する必要はない。今回の検証では、MAC アドレスを用いて端末ごとに制限を掛け、疑似的に図 11 のように最大ホップ数が 1 ホップのダイヤモンド型を構築した。周辺に未認証の学生がいない場合、5 秒過ぎると、タイムアウトとなり、講師側へ返送するという設定にした。

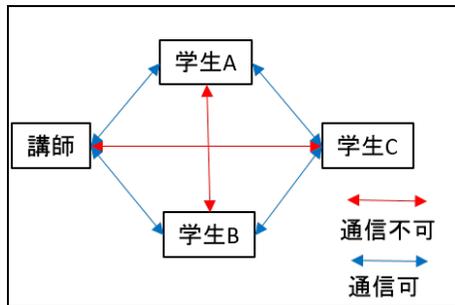


図 11 ダイヤモンド型の構成図

結果として、講師が送信し始めて、学生からの受信を終えるまで約 8 秒掛かった。タイムアウトの時間は 5 秒なので、1 ホップに 3 秒掛かったことになる。図 13 の 900 m<sup>2</sup>の最大ホップ数は約 7 ホップなので約 21 秒、タイムアウトの 5 秒を含めて約 26 秒掛かる計算となる。

## 5. まとめ

本論文では、専用の機器を用いないことで導入コストを低くし、Bluetooth を用いることで出席確認の範囲をより限定し、屋外でも利用可能なシステムを提案した。今回のシミュレーションと実機検証から、900 m<sup>2</sup>の講義室で提案システムを用いた場合の出席確認には約 26 秒かかることが分かった。この数値は出席確認にかかる時間として、講義の妨げにはならないと考えられ、提案システムを用いて出席確認をすることが可能であることを確認した。今後の課題として、本来学生は一人ひとりランダムに座るのではなく、ある程度友人たちと固まって座るのが現状である。そこでシミュレーションでは意図的に学生を固まらせて配置した場合の検証も行っていく。

## 参考文献

- 1) Bokrae Jang, Jaegeol Yim, Seung-Hyun Oh: A Review of Attendance Management Systems, Advanced Science and Technology Letters Vol.143 (AST 2017).
- 2) Jin Kim and Seung-Kook Cheong: Research on an Authentication Algorithm for an Electronic Attendance System in the Constructing of a Smart Campus, International Journal of Security and Its Applications Vol.7, No.6 (2013).
- 3) 鶴川義弘, 福井恵子, 上山由果, 安藤明伸, 黒川修行, 鉄本良, 藤井俊彰, 岩田薫, 今野幸典, 藤沢和繁, 高橋修: 無線 LAN アクセスポイントを用いる出席管理システム, 宮城教育大学情報処理センター研究紀要第 25 号(2018).

- 4) 嶋川司: BLE ビーコンを用いた出席確認, 第 172 回月例発表会(2016 年 8 月).
- 5) 輿大輔: 携帯電話の GPS 機能を用いた出席管理システムの有効性に関する考察:近畿大学での測位データ分析を基に, 商経学叢第 58 巻第 2 号(2011 年 12 月).