偽造 Wi-Fi アクセスポイントによる現在地情報のスプーフィング攻撃の脅威

江藤 一樹

明治大学総合数理学部 先端メディアサイエンス学科 菊池研究室

1 はじめに

近年，スマートフォンの普及に伴い，ゲームや食事サイトなどのインターネットサービスで，デバイスを通して取得される位置情報の利用が増え，社会インフラとして必要性が高まった．その一方，GPS（グローバル・ポジショニング・システム）への悪意ある攻撃として，スプーフィング攻撃（なりすまし攻撃）の脅威が指摘されている [1]．これを受けた GPS は実際にいる位置とは異なる位置を示し，船の自動運転やドローンなどの社会インフラの混乱を引き起こす原因となる．2018 年 11 月 12 日に，店舗に訪れたかのように位置情報を偽り，イオンアプリの来店ポイントを不正取得したとして，男が逮捕された [2].

デバイスは，周囲にあるアクセスポイント（AP）の MAC アドレスをサーバに送信し，AP の情報が格納されているデータベースと照合して，位置情報を推定する．従って，偽装された偽の MAC アドレスを与えられるとデバイスの現在位置を操作されてしまう恐れがあると考えられる．

そこで，本稿ではこの位置情報のスプーフィング攻撃の実現可能性を調査し，攻撃のリスクと攻撃を受ける条件を明らかにする．攻撃の検証の為に，Ubuntu 18.04 LTS が搭載された PC を 5 台用意し，ネットワークインターフェイスの MAC アドレスを偽装する．

本研究の新規性は次の通りである．

1. デバイスに対する位置情報のスプーフィング攻撃のリスクを明らかにすること．
2. 偽 AP の信号強度などの条件を明らかにする．
3. 位置情報スプーフィング攻撃への対策．

2 提案手法

本研究で検証する位置スプーフィング攻撃は，攻撃対象のデバイス付近に，異なる場所にある AP の MAC アドレスを偽装した偽の AP を複数設置することにより，現在位置を誤推定させることで実現する．

実験システムの概要図を図 1 に示す．偽の ARP パケット a_3，a_4，a_5 を受信したホストは，本来の a_1，a_2 よりも a_3 付近の位置と誤認する．

2.1 Geolocation API[3]

W3C（World Wide Web Consortium）によって標準化された，Web からデバイスの位置情報を取得する API である．JavaScript の navigator.geolocation オブジェクトを通じて提供される．デバイスがこのオブジェクトに対してメソッドを実行する時に，実行したデバイスの IP アドレス，周囲の Wi-Fi の MAC アドレス，GPS の情報などを API を介して，サーバーにリクエストを送り，位置情報を取得する．Geolocation API を使用するには，通信が https であることが必須であるため，サーバに送られている内容を盗聴することを困難にしている．

2.2 MAC アドレスの偽装

ネットワークインターフェイスの MAC アドレスを任意な値に変更する Linux のパッケージである macchanger[4] を使用する．図 2 は，macchanger によって偽装された偽 AP の MAC アドレス aa:aa:bb:bb:cc:cc を含む ARP パケットである．

2.3 AP 情報の取得

AP の数と情報を取得する為に，macOS の “airport” コマンドを使用する．このコマンドは，デバイス周辺にある AP の SSID，MAC アドレス，信号強度，チャンネルを含む 7 つの情報を表示する．

3 実験

位置情報の偽装が可能な条件を調べるために，以下の条件で実験を行う．

1. 実験 1 : PC とスマートフォンによる位置情報の観測とスプーフィング実験．
2. 実験 2 : 偽 AP と対象デバイスの距離，AP の数についてのスプーフィング実験．

†Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University, Kikuchi Laboratory.

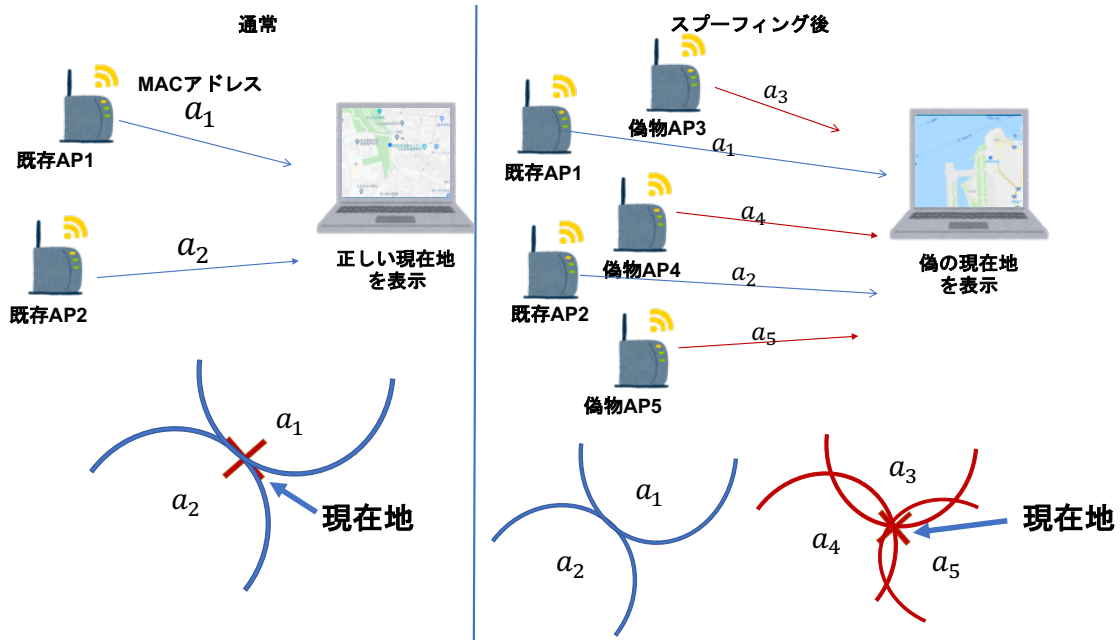

図 1　提案手法の概要図

No.	Time	Source	Destination	Protocol
506	3.615480	MS-NLB-PhysServe…	Broadcast	802.11
507	3.635397	NecPlatf_25:ad:d0	Broadcast	802.11
508	3.648389	aa:aa:bb:bb:cc:cc	Broadcast	802.11
509	3.651552	NecPlatf_aa:09:4a	Broadcast	802.11
510	3.664128	Buffalo_06:9f:3f	Broadcast	802.11
511	3.666624	OkiElect_87:12:71	Broadcast	802.11

```
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: aa:aa:bb:bb:cc:cc (aa:aa:bb:bb:cc:cc)
Source address: aa:aa:bb:bb:cc:cc (aa:aa:bb:bb:cc:cc)
BSS Id: aa:aa:bb:bb:cc:cc (aa:aa:bb:bb:cc:cc)
```

図 2　MAC アドレスを偽装した ARP パケット

3.1　実験環境

位置スプーフィング攻撃が成功するためには，既に存在する AP 数を上回る必要があると仮定し，偽 AP を 5 台用意する．偽 AP の MAC アドレスは，異なる場所にある周囲の AP から，攻撃者が信号強度の強い順に 5 台選択し，それぞれの MAC アドレスに偽装する．

3.2　偽装対象のインターネットサービス

本研究では，ユーザの現在地を地図上に表示する次の 2 つのサイトを利用する．Googole 社が提供している地図サービス “Google Maps”．すかいらーくグループの公式サイトが提供している「ガスト店舗検索」サービスである．

3.2.1　地図 API を使用したサイトの調査

地図 API を使用している主要サイトの中で Geolotion API を利用しているサイトの割合を調査した．305 件調べ，Geolocation API を利用有無の結果を表 1，地図 API の種類別の利用頻度を表 2 に示す，に示す．305 件中，Geolotion API を使用してるサイトは 18 件である．そのうちの 17 件はユーザの周辺にある店舗検索に利用されており，残りの 1 件がすかいらーくグループの公式サイトである．

3.3　実験方法

3.3.1　実験 1：PC とスマートフォンを用いた位置情報の観測

実験 1 では，GPS の有無，異なるインターネットサービスで偽装結果に変化があるのか調べる．そのために，GSP が搭載されているスマートフォンと搭載されていない PC で検証する．現在地を取得する際，デバイスをオンラインとオフラインの二つの状態にする．実験条件を表 3 に示す．

観測場所は，本研究室，自宅，江古田の森公園付近，本学地下室の四箇所である．偽 AP が偽装する MAC アドレスは，東京都小金井市のたけのこ公園付近で入手した AP の MAC アドレスである．

既存 AP と偽 AP の数の関係性を明らかにする為，実験場所の AP 数を調べる．5 秒間隔で，PC を用いて AP

表 1　Geolotion API の有無

サイト名	API	Geolotion API の有無
Hot pepper グルメ	Google Maps	無
マクドナルド	Google Maps	有
スターバックス	MAPPLE	有
すかいらーくグループ	Google Maps	有
⋮	⋮	⋮
Retty	Yahoo map API	無
計		18/305

表 2　地図 API 別の利用頻度

Google Map API	274
いつも NAVI	12
Yahoo map API	7
その他	12

表 3　実験条件

	機種	オフライン	オンライン
スマートフォン	iPhone SE（IOS 12.4.1）	機内モード	LTE or Wi-FI 接続あり
PC	Macbook Pro（macOS Catalina）	接続なし（Wi-Fi off）	デザリング or Wi-Fi 接続あり

の数を 100 秒間取得する．一つの AP がチャンネル毎に異なる MAC アドレスを所持している場合，その MAC アドレスの数を AP の数とする．

本実験では，他の場所の AP の MAC アドレスに変えて位置情報の偽装がされるか調べる．偽装に使用する AP は，京都府にある法然寺付近と沖縄県の那覇空港，香港の三ヶ所である．攻撃対象を PC のみ，実験場所を本学地下室，偽 AP の数を 5 台とする．

3.3.2　実験 2 : 偽 AP と攻撃対象デバイスの距離，偽 AP の数による影響

環境を変えて調査を行い，位置情報の偽装がされるか調べる．偽 AP と攻撃対象の距離を 0m，3m，6m，9m，12m と変化させた時の信号強度と位置情報の偽装結果を調べる．信号強度は，50 秒間に 10 回取得し，その結果の平均とする．

偽 AP と攻撃対象の距離を 0m にし，偽 AP の数を 5~1 まで変化させて，位置情報が偽装されるか否かを調べる．

表 4　実験場所の AP 数

場所	AP の数	
	μ	σ
研究室	123	11.8
自宅	63	4.8
公園	19	4.8
地下室	2	0.4

3.4　実験結果

3.4.1　実験 1

実験場所の AP 数を表 4，位置スプーフィング結果を表 5 に示す．ここでの〇は偽装できたこと，×は正常の位置推定が行われたことを示す．

表 5 より，位置スプーフィング攻撃が成功したのは，本学地下室で PC を対象とした時だけで，実験条件での結果に違いはない．その為，位置情報の偽装に最も関係する条件は，既存 AP と偽 AP の数である．

スマートフォンに対する位置情報の偽装は，実験環境によらず，されないことが分かった．AP の情報ではなく，GPS か携帯基地局のセンサーに基づいて位置を推定

表 5　実験 1 の位置スプーフィングの結果

デバイスの状態	GPS	実験場所	Google Map	すかいらーく
オンライン	あり	研究室	×	×
		自宅	×	×
		公園	×	×
		本学地下室	×	×
	なし	研究室	×	×
		自宅	×	×
		公園	×	×
		本学地下室	○	○
オフライン	あり	研究室	×	×
		自宅	×	×
		公園	×	×
		本学地下室	×	×
	なし	研究室	×	×
		自宅	×	×
		公園	×	×
		本学地下室	○	○

表 6　実験結果

AP 元の場所	Google Maps	すかいらーく
京都	○	○
沖縄	○	○
香港	○	○

図 3　実験 1 の偽装結果（那覇）

図 4　実験 1 の偽装結果（香港）

している と考えられる．

位置スプーフィングされた偽装結果を図 3（すかいらーく）と図 4（Google Maps）に示す．両サイトで同じ場所を指したことから，Geolotion API を利用しているサービスに対して，位置情報の偽装がされると分かった．

3.4.2　実験 2

偽装対象のデバイスと偽 AP の距離を変えた位置スプーフィングの結果を表 7，偽 AP 数を変えた結果を表 8 に示す．ここでの○は位置情報が偽装されたこと，×は正常の位置推定が行われたことを示す．両結果から位置情報の偽装に必要なのは，既存 AP 数より多い偽 AP 数を設置することだと分かる．

3.5　考察

3.5.1　実験 1：観測

GPS ありのデバイスの位置情報は，実験環境によらず偽装されない．GPS の電波が届きにくい地下室の実験では図 5 の様に，位置情報の精度は悪くなるが，実験場所付近を指している．従って，位置情報の推定には，AP の結果より GPS の結果を優先していることが分かる．

オンラインに接続をしていない状態でも正常の位置を指した．これはブラウザにキャッシュされた情報から位置を推定していると考える．

表 7　距離を変えた実験結果

結果	距離 [m]	偽 AP										既存 AP			
		a[dBm]		b[dBm]		c[dBm]		d[dBm]		e[dBm]		a'[dBm]		b'[dBm]	
		μ	σ	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ
○	0	-36.4	0.68	-39.8	2.6	-35.2	2.2	-32.3	4.3	-41.7	1.2	-89.2	1.2	-90	1.5
○	3	-55.6	4.1	-54.2	2.0	-58.7	2.7	-51.7	2.9	-56.3	1.8	-85.4	1.9	-85.6	1.4
○	6	-63.6	1.8	-56.1	2.6	-57.8	2.9	-56.6	1.6	-61.8	2.0	-86	3.2	-85.6	3.1
○	9	-66	1.4	-66.6	0.5	-64.4	1.8	-60.9	1.4	-59.3	1.4	-88.6	1.0	-88.1	2.6
○	12	-69.3	1.8	-61.1	2.4	-65.1	1.0	-57.4	1.7	-64.6	2.1	-87.4	1.9	-87.4	1.6

表 8　偽 AP 数を変えた実験結果

結果	偽 AP 数
○	5 台
○	4 台
○	3 台
○	2 台
×	1 台

図 5　スマートフォンを用いた地下室での観測結果

3.5.2　実験 1：PC による実験

表 6 より，位置情報の偽装がされる場所は，AP の MAC アドレスがデータベースに格納されていれば，どこでも可能だと考える．両サイトによる結果に違いがなかったのは，使用しているブラウザが同じな為，照合を行っているデータベースも同じだからと思われる．

この実験により，第三者の位置情報に対する偽装だけでなく，[2] のニュースのように自身のデバイスの位置情報を全国各地に偽装し，不正に利益を得ることができてしまうことが現実的であることが実証された．

3.5.3　実験 2

既存 AP の信号強度は非常に弱い電波であるが，既存 AP が偽 AP の数を上回った時に，実験場所付近を指したことから，位置スプーフィングに信号強度が関係しないと考える．その為，電波を拾えれば 12m より距離を離しても偽装がされてしまうリスクがある．

4　対策

本リスクへの対策は以下である．

1. GPS の使用を必須にする
2. 多様なリソースからの推定
3. キャッシュ，履歴からの推定

本研究で，GPS が搭載されているデバイスに対する位置情報の偽装がされなかったことが示された．従って，ドローンや自動運転の乗り物などの位置情報を利用したデバイスに対し，GPS を搭載することが効果的である．しかし，GPS の信号が受信できない環境から安全に位置推定をするために，Wi-FI などの位置情報に使えるリソースを複数組み合わせる必要がある．スプーフィング攻撃により位置情報が急に変化した時，変化前のキャッシュや履歴から現在地を推定するか，ユーザに対して「位置情報が偽装されている可能性がある」等の警告を送るべきと考える．

5　おわりに

本研究では，インターネットサービスで利用される現在地を取得する機能に対して，位置情報のスプーフィング攻撃の実現可能性を調査し，攻撃のリスクと攻撃を受ける条件を明らかにした．位置情報の取得には，デバイス周辺にある AP の MAC アドレスが利用されていることから，既存 AP の数を上回る MAC アドレスを偽った AP を設置することで，GPS を搭載していないデバイス

の位置情報が偽装されると分かった．香港や那覇への偽装がされたことから，AP の MAC アドレスがデータベースに格納されていれば，偽装される場所には，制限がない．このリスクに対する対策として，GPS の使用を必須にする，多様なリソースからの位置推定，キャッシュ，履歴からの推定の三つが考えられる．

今後の課題は，以下の三つである．

1. 異なるブラウザによる観測
2. 既存 AP と偽 AP を同数にした実験
3. サーバに送る内容を明らかにする

Google や Apple などのブラウザを提供している企業は，それぞれで AP の MAC アドレスと位置情報を紐づけたデータベースを構築している．その為，Geolotion API を実行した際，各ブラウザはそれぞれの企業が所持しているデータベースと照合していると予想する．そこで，照合を行うデータベースが異なるか調査し，位置スプーフィング攻撃のリスクを受けるデータベースを明らかにする．

実験 2 で，偽 AP が既存 AP の数を上回っている場合，位置情報の偽装がされると分かったが，偽 AP と既存 AP を同数にした場合，位置情報の偽装に信号強度が関係するのか明らかになっていない為，調査する必要がある．

参考文献

[1] 海老沼，”GPS 信号の脆弱性と今そこにある危機”，中部大学工学部紀要，2017.

[2] イオンから来店ポイント詐取容疑　ＰＣで位置情報偽装（https://www.asahi.com/articles/ASLCD6R60LCDTIPE03N.html?ref=newspicks，2019 年 12 月参照）

[3] Geolocation API Specification 2nd Edition（https://www.w3.org/TR/geolocation-API/，2019 年 12 月参照）

[4] ubuntu manuals（http://manpages.ubuntu.com/ manpages/bionic/man1/macchanger.1.html，2019 年 12 月参照）

[5] Google の位置情報サービスに登録されたアクセス ポイントを管理する（https://support.google.com/maps/answer/1725632?hl=ja　2019 年 12 月参照）