



Södra Latins gymnasium, Stockholm

Åke Amcoff

Jarl Åkesson

12 april 2024

Passiv lokalisering av wifi klienter

Handledare: Rickard Fors

Sammanfattning

Hela tiden platsbestäms vi, och platsdata samlas in av appar som Google Maps för att till exempel mäta mängden trängsel på restauranger eller fordonstrafik. Denna platsbestämning sker genom GPS-system inuti enheterna där deras position avgörs genom trilaterering. Problemet med denna metod är att avsändarna själva avgör när de vill skicka in information till en databas. Platsbestämning av enheter utan detta självrapporтерingsbehov skulle möjliggöra mer omfattande statistik angående platsdata. Syftet med detta gymnasiearbete är att undersöka hur rimlig denna form av lokalisering av wifiklienter är avseende vilken precision som kan uppnås.

För att undersöka detta omprogrammerade vi mjukvaran i en Asus RT-AC86U wifirouter i syfte att mäta fasförskjutningen av signaler från en wifiklient mellan routerns tre externa antenner och på så sätt beräkna precisionen möjlig vid triangulering med denna router – som är en tämligen typisk ”off-the-shelf”-router, vilket är avgörande för om ett system baserat på denna rapport kan implementeras i existerande wifinätverksinstallationer.

I experimentet uppnåddes en precision om i genomsnitt $(\pm 0.77)^\circ$ för vinklar mellan -30° och 30° . På grund av antennernas placering på routern kunde inte större vinklar mäts.

Abstract

We are localised all the time, and location data is collected by applications such as Google Maps in order to measure crowdedness at restaurants, or traffic levels, for example. This localisation is done using the built-in GPS systems of the devices, which in turn utilise satellites and trilateration to determine the location of the devices. The main issue with this method is that it builds upon *active* localisation, meaning that the devices being localised themselves need to report their location, as opposed to *passive* localisation where the position of the devices can be silently detected by a third party. Passive localisation would thus enable more thorough location statistics. The purpose of this paper is to determine the level of precision achievable with such a passive localisation system.

In order to study this, we reprogrammed the firmware of an Asus RT-AC86U wifi router to be able to measure the phase shift between the router’s three antennas of wifi signals originating from a wifi client in order to determine the angle of arrival of the signal, and in turn the direction of the wifi device itself. A crucial property of the wifi router used in this study is that it is a very typical, off-the-shelf router, which means a system based on this paper could be deployed widely at low cost.

An average precision of $(\pm 0.77)^\circ$ for angles between -30° and 30° was achieved in the experiment. The manufacturer’s antenna placement prohibited the measuring of larger angles.

Tillkännagivanden

Genom Norrnässtiftelsen blev vi tilldelade pengar från Södra Latin av summan 1 000 kronor. Utan detta hade inköp av nödvändiga materiel varit omöjlig.

Genom sitt överseende tillät Jenny Alpsten programmering av gymnasiearbetet under ett flertal mattelektioner. Utan detta är det oklart huruvida ett genomförande av vårt experiment hade varit möjligt inom den givna tidsramen.

Vidar Nordqvist var en kämpe och gav emotionellt stöd vid inköp av wifiroutern Asus RT-AC86U från Blocket. Med rädsan närvarande vid inköp genom Blocket i åtanke, var detta starkt och hjälpsamt.

Innehåll

1 Inledning	4
1.1 Presentation	4
1.2 Syfte	4
1.3 Frågeställning	5
2 Bakgrund	6
2.1 Triangulering och trilaterering	6
2.2 (Trådlös) kommunikation mellan nätverksenheter	7
2.3 Ortogonal frekvensdelningsmultiplex	8
2.4 Interferens och fasförskjutning	8
2.5 Channel state information	11
3 Metod	12
3.1 Materiel	12
3.2 Avgränsningar	12
3.3 Genomförande	13
4 Resultat och analys	15
5 Diskussion	17
6 Slutsats	17
7 Bibliografi	18

1 Inledning

1.1 Presentation

Sedan början av 1970-talet har GPS (*Global Positioning System*) blivit en alltmer använd teknologi. Det fungerar genom att ett flertal satelliter skickar ut information cirka 20 000 kilometer från jorden med hjälp av transpondrar om sin exakta tid och position. GPS-mottagaren (installerad i en mobiltelefon, till exempel) får då in information från flera satelliter och kan genom *trilaterering* räkna ut exakt var den är. Trilaterering är ett sätt att fastställa en enhets position genom att mäta avståndet från enheten till tre eller fler andra enheter (se Kapitel 2.1). Eftersom det finns minst fyra satelliter ovanför ett GPS system fungerar detta alltid¹. (Lantmäteriet, u.å.)

Idag platsbestäms vi hela tiden, och platsdata samlas in *en masse* av appar som Google Maps för att till exempel uppskatta hur trafikerad en väg är eller hur lång en restaurang är – i realtid. Denna funktion bygger på självrappportering. Wifienheter vet genom GPS sin position och ger den informationen till Google som sedan drar slutsats om trafikering. Eftersom denna metod är beroende av självrappportering avgör enheten själv när dess information bör sändas till en databas. Detta skiljer sig från *passiv lokalisering* där en sensor avgör var en enhet är utan att någon åtgärd krävs från användarens enhets håll.

Problemet med passiv lokalisering är att det potentiellt strider mot dataskyddsförordningen på ett flertal punkter. För att behandling av personuppgifter ska vara laglig måste den stödja sig på minst en av förordningens sex rättsliga grunder. Ifall en omfattande insamling av platsdata som enbart går att genomföras utan aktiv tillåtelse från varje enhets ägare faller inom ramen av allmänt intresse skulle det till exempel vara lagligt. Om det vore lagligt skulle det ändå krävas mycket resurser för att säkerställa att alla personuppgifter hanteras korrekt vilket kan vara mer kostsamt än användbart. Eftersom dataskyddsförordningen gäller i hela EU är det heller inte rimligt att den kan förändras för att tillåta passiv lokalisering på stor skala.

Fastställning av position är dock inte bara möjligt genom trilaterering. Istället för distans och tid kan det genom *triangulering* platsbestämmas. I denna metod mäts vinkeln mellan avsändare och minst två mottagare. Om mottagarnas exakta positioner är kända kan avsändarens plats bestämmas. Eftersom tid inte är en variabel som beräknas är atomklockor inte nödvändiga för platsbestämning genom triangulering vilket gör denna metod billigare och enklare för undersökningar på en mindre skala än motsvarande trilatereringsmetod, när det rör sig om radiosignaler, vars hastighet är så hög (c) att skillnaden i ankomsttid mellan mottagare kan vara bara några nanosekunder.

1.2 Syfte

Syftet med detta gymnasiearbete är att undersöka om passiv platsbestämning av wifienheter är träffsäkt och rimligt. Ifall detta är rimligt skulle det innebära möjligheter för större insamling av data att användas under effektivisering av stadsplanering samt egentid.

Problemet med *aktiv platsbestämning* är att den är beroende av självrappportering. Alltså avgör enheter själva när information om deras position är lämplig att sända till en databas. På grund av att enheterna själva avgör när platsbestämning är lämpligt ger inte detta lika omfattande statistik som platsbestämning utan aktiv tillåtelse. Ifall hög precision kan uppnås genom passiv platsbestämning skulle detta ha många tillämpningsområden inom effektivisering av stadsplanering.

Den mer omfattande mängden data skulle innebära enklare identifiering av trafikering. Butiksägare och restaurangägare kan då bättre optimera öppettider och marknadsföring för att minska konkurrens samt öka tillgänglighet. Det skulle också göra livet enklare för konsumenter, eftersom de alltid hade vetat väntetider för restauranger eller trängsel i butiker och mataffärer vilket skulle innebära

¹Förutsatt att GPS-signalerna når mottagaren och inte blockeras av tjocka betongväggar eller dylikt.

en minskning i slöseri av tid. Uppskattningar av fordonstrafik skulle också vara mer korrekta vilket hade möjliggjort mer effektiv infrastruktur, eftersom problematiska områden och tidpunkter då är mer uppenbara.

Problematiska områden avseende smittspridning vore också enklare att identifiera. Vid utbrott av aggressivt smittsamma sjukdomar skulle mer effektiv samt större mängd platsdata möjliggöra för områdesspecifika restriktioner och då minska behovet av omfattande restriktioner samt mängden drabbade av sjukdom. Privatpersoner hade då mer enkelt kunnat ta del av nödvändiga aktiviteter som inhandling av livsmedel samt mindre nödvändiga aktiviteter som restaurangbesök vilket hade lett till att färre företag måste stänga ner eller göra nedskärningar.

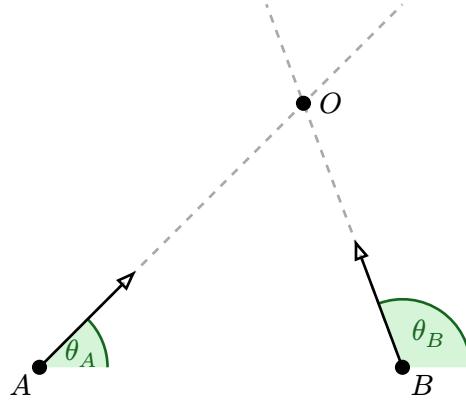
1.3 Frågeställning

Vilken precision kan uppnås vid bestämning av en wifienhets riktning med en wifirouter märkt Asus RT-AC86U?

2 Bakgrund

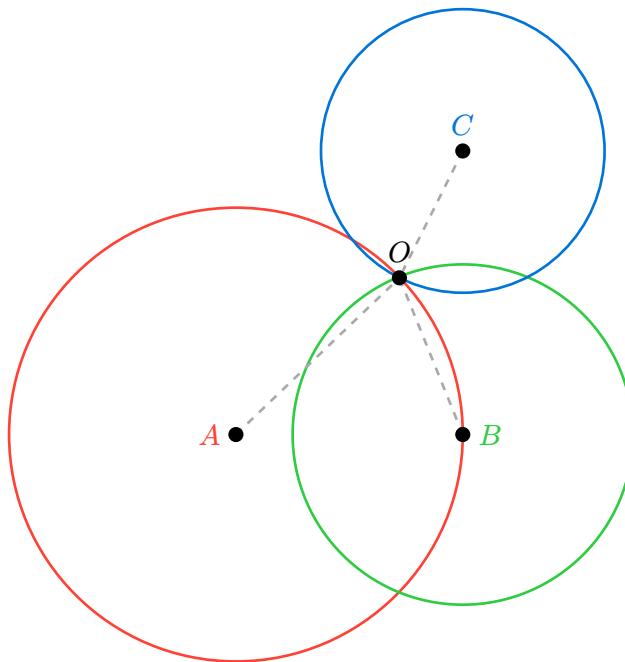
2.1 Triangulering och trilaterering

Triangulering och trilaterering är två olika sätt att placera bestämma något (här: O) genom att mäta vinklar respektive avstånd. Båda kräver flera mätningar från olika punkter vars positioner är kända (här: A, B, C).



Figur 1: Triangulering av O från A och B .

Med två kända punkter A och B , samt vinkeln till O från respektive punkt, går det att triangulera O . Varje vinkel ger en stråle (de streckade linjerna i Figur 1) varpå O kan ligga. Där strålarna från A och B korsar varandra finns O .



Figur 2: Trilaterering av O från A, B och C .

Trilaterering kräver avståndsmätningar till en okänd punkt O från minst tre punkter (A, B och C). Avståndsmätning till O från A ger en sträcka $|AO|$, och alla punkter som ligger på avståndet $|AO|$ från A utgör kanten på en cirkel med radien $|AO|$; dessa punkter är alla möjliga positioner för O . När avståndet mäts på samma sätt från B till O får en ytterligare cirkel, och de möjliga positionerna för O begränsas till de två skärningspunkterna mellan cirklarna. För att begränsa antalet möjliga positioner till en enda krävs en tredje mätning, C . I den gemensamma skärningspunkterna för alla tre cirklar finns O .

2.2 (Trådlös) kommunikation mellan nätverksenheter

Det finns en rad olika standarder och protokoll som nätverksenheter² använder för att kommunicera med varandra. De mer abstrakta (icke-fysiska) protokollen, som HTTP (för webbsurfning) och SMTP (för mejl), gör ingen skillnad på om de förs över wifi eller trådbundet. Likaså spelar det ingen roll för wifikretsen huruvida bitarna som sänds och tas emot är HTTP, SMTP, nonsens eller något annat. I grund och botten handlar de flesta internetprotokoll om att representera information i binär form (i bitar) på ett eller annat sätt. De mest grundläggande protokollens syfte är att överföra dessa bitar genom den fysiska världen, till exempel genom en kopplarkabel eller i luften.

OSI-modellen, framtagen av ISO Central Secretary (1994), är ett försök att kategorisera standarderna för kommunikation nätverksenheter sinsemellan, och tanken är att varje *lager* ska vara helt oberoende av de andra lagren och att lagren ska kunna kombineras obehindrat. HTTPS (HTTP Secure), till exempel, heter *secure* eftersom det är krypterat, men namnet är missvisande eftersom informationen inte krypteras i HTTP(S)-lagret (lager 7) utan i lager 6, med TLS. HTTP, å andra sidan, är okrypterat och sålunda inte ”inneslutet” av TLS i lager 6. På lager 7 är HTTP och HTTPS dock identiska, vilket gör att mycket HTTP-programkod (webbservrar, till exempel) kan nyttjas oavsett om kryptering används eller ej.

Lager	Använts till	Exempel
7 Applikation	Applikationsprotokoll	HTTP
6 Presentation	Kompression, kryptering, teckenkodning	TLS
5 Session	Sessionshantering	SOCKS
4 Transport	Sändnings- och ankomstkontroll	TCP
3 Nätverk	Logisk adressering	IP
2 Datalänk	Fysisk adressering	MAC
1 Fysisk	Bitöverföring	IEEE 802.3, IEEE 802.11

Tabell 1: OSI-modellens lager.

Lager 1 överför bitar genom den fysiska världen. IEEE 802.3 (Ethernet) och IEEE 802.11 (wifi) hör till de mest kända samlingarna av standarder; IEEE 802.3 standardiseras bitöverföringen i kopplarkabler och fiberoptik medan IEEE 802.11 standardiseras trådlös överföring.

Wifigeneration	IEEE-standard	Antagen
(Wifi 0) ³	802.11	1997
(Wifi 1) ³	802.11b	1999
(Wifi 2) ³	802.11a	1999
(Wifi 3) ³	802.11g	2003
Wifi 4	802.11n	2008
Wifi 5	802.11ac	2014
Wifi 6	802.11ax	2019
Wifi 7	802.11be	2024
Wifi 8	802.11bn	2028

Tabell 2: IEEE 802.11-standarder och motsvarande konsumentvänliga namn. (Phillips, 2023)

²Med ”nätverksenheter” avses mobiltelefoner, datorer, servrar, routrar med mera; allt som är uppkopplat till internet och lite till.

³Wifi 0 … 3 är inofficiellt och retroaktivt namngivna.

IEEE 802.11 består av en uppsjö standarder från de senaste 30 åren. I vårt experiment studeras IEEE 802.11ac (den näst senast antagna standarden) av två huvudsakliga skäl: Dels är IEEE 802.11ac-kretsar i skrivande stund vanligt förekommande och relativt billiga jämfört med IEEE 802.11ax-kretsar, dels är verktyget för manipulering av wifikretsmaskinvara som utvecklades av Gringoli m.fl. (2019) designat för IEEE 802.11ac.

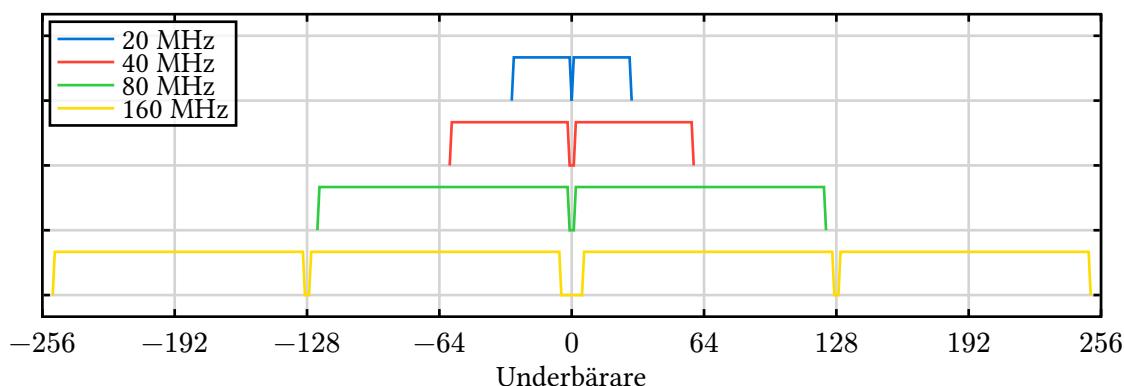
IEEE 802.11 är en komplicerad standard, men det enda som läsaren behöver ta med sig är följande:

- Wifisignalerna skickas på en viss *kanal* (del av frekvensspektrumet⁴) som bestäms av wifiroutern som enheten är ansluten (eller försöker ansluta) till.
- Bitarna som lagret ovanför (lager 2) vill överföra paketeras i *wififramar* och skickas några (upp till 2 304 bytes) i taget, tillsammans med mottagaradress och en del ytterligare information som är irrelevant här. Ju fler bitar, desto fler wififramar.
- I denna studie har wifisignalen den ungefärliga frekvensen 5 GHz.

2.3 Ortogonal frekvensdelningsmultiplex

Ortogonal frekvensdelningsmultiplex (OFDM) ökar överföringshastigheten genom att signalöverföringen delas in i flera parallella dataströmmar, så kallade underbärare (*subcarriers*), på var sin frekvens. OFDM gör signalöverföringen tålig mot störningar som drabbar vissa frekvenser, och dessutom kan de olika underbärarna reflekteras på olika sätt så att *tillräckligt många* når mottagaren. (Weinstein, 2009)

OFDM används i alla wifistandarder från och med IEEE 802.11a (Phillips, 2023), och således även i IEEE 802.11ac som granskas ingående i denna rapport.



Figur 3: Underbärare som används i IEEE 802.11ac för varje bandbredd. Glappen (vid 0, till exempel) orsakas av oanvända underbärare. Varför vissa underbärare inte används är irrelevant här.

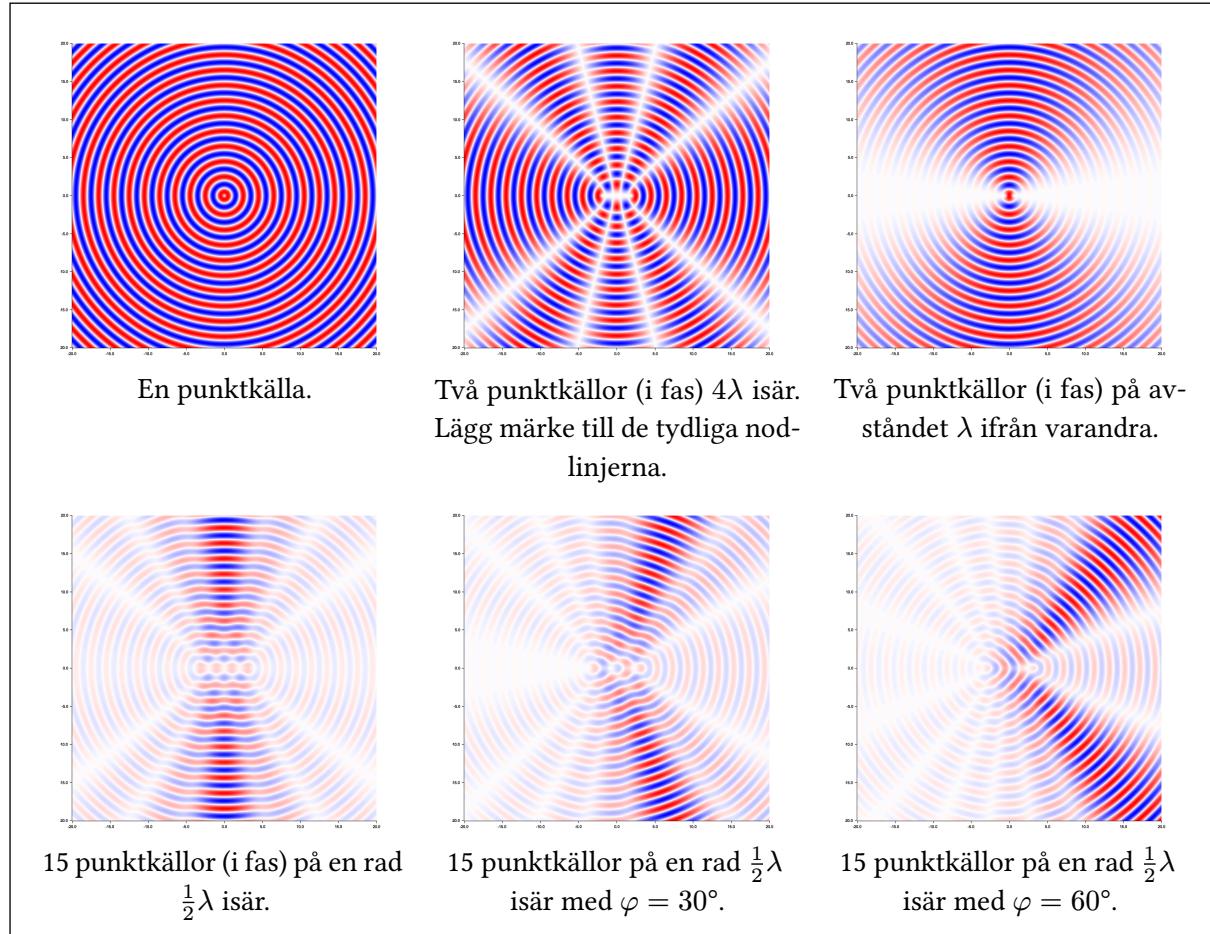
Figur 3 visar underbärarna för olika *bandbredder* (20, 40, 80 respektive 160 MHz), det vill säga olika stora ”block” av frekvensspektrumet⁴. Underbärarna i IEEE 802.11ac är vanligtvis placerade 312,5 kHz isär (Phillips, 2023) – i Figur 3 har underbärare k frekvensen $f_0 + k \cdot 312,5 \text{ kHz}$ där f_0 är den mittersta underbäraren (underbärare 0) frekvens; *centerfrekvensen*.

2.4 Interferens och fasförskjutning

I moderna wifiroutrar används flera antenner. Tillsammans bildar antennerna ett antennsystem där varje antenn utgör ett så kallat element. Om antennerna är uniformt fördelade längs en linje bildar de ett uniformt linjärt antennsystem (*ULA*; *Uniform Linear Array* på engelska); se Figur 5. Routern som används i experimentet har ett uniformt linjärt antennsystem med tre element (vilket framgår i Figur 7).

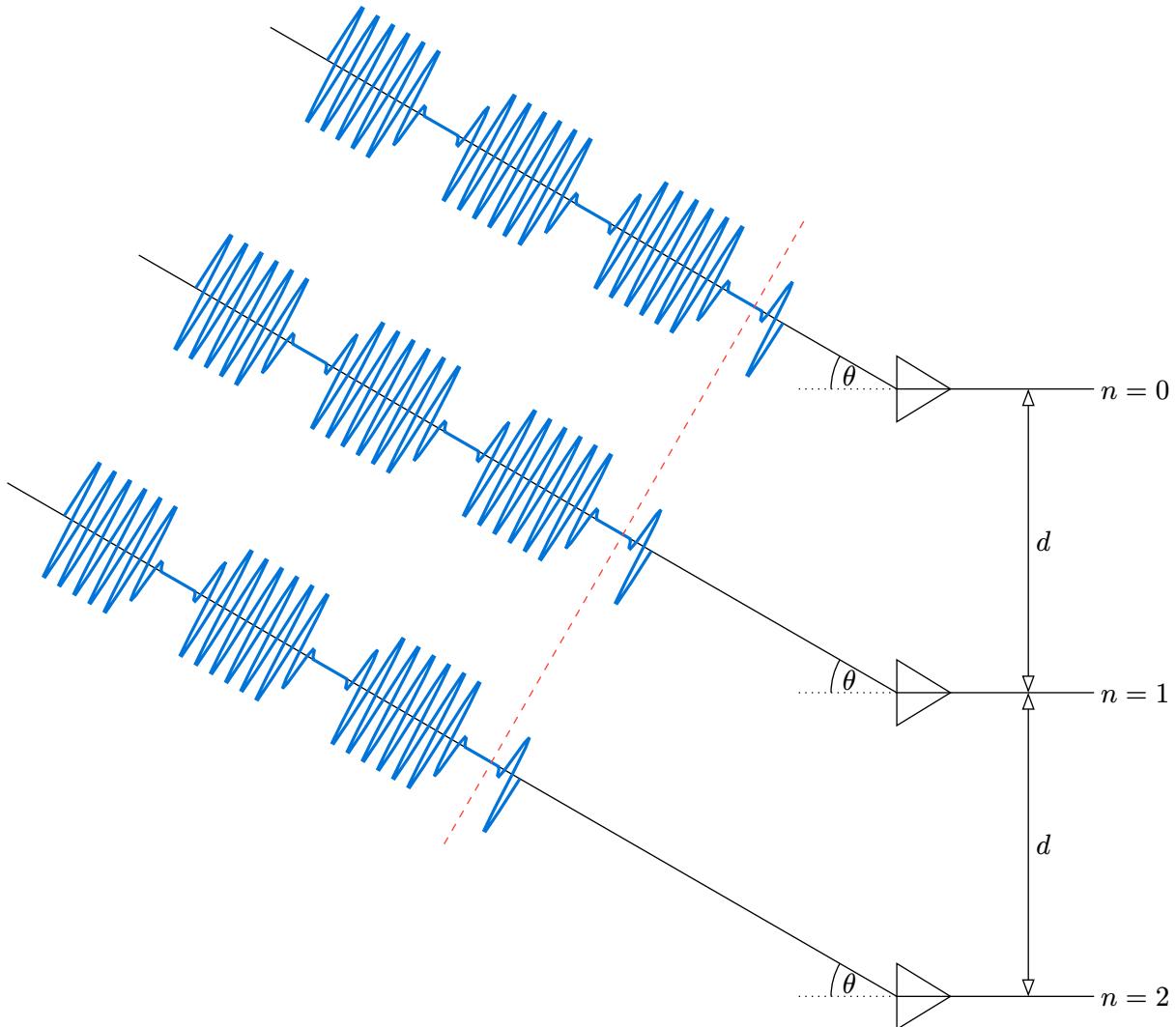
⁴I EU har frekvensbandet (5,150 till 5,875) GHz allokerats till wifi (Phillips, 2023).

En sändare kan införa en viss fasförskjutning φ mellan intilliggande antennelement och utnyttja interferens för att rikta signalen åt ett visst håll (så kallad *beamforming*). Figur 4 illustrerar detta. En mottagare kan på motsatt sätt bestämma den infallande signalens vinkel θ utifrån den uppmätta fasförskjutningen mellan angränsande element.



Figur 4: Interferensmönster för olika sorters linjära antennsystem. Våglängden λ är 1 l.e. och färgningen visar den relativna (i respektive diagram) elongationen i varje punkt – blått är negativt, vitt är noll och rött är positivt.

För att θ ska kunna bestämmas precis måste signalen i fråga träffa alla antennelement från samma vinkel, och källan måste alltså befina sig på ett tillräckligt stort avstånd från antennsystemet så att vågfronterna blir någorlunda parallella och i fas.



Figur 5: Uniformt linjärt antennsystem med tre element. Den infallande signalen (som ser ut att vara tre separata signaler men som inte är det) har vinkeln θ och källan antas befina sig på ett så stort avstånd D från antennerna att signalen träffar alla antennelement från ungefär samma vinkel ($D \gg d$).

Betrakta den rätvinkliga triangel vars hypotenusan (med längden d) går mellan två intilliggande antenner och vars ena katet är ortogonal mot den infallande signalens riktning. Triangelns andra katet kommer ha längden

$$x = d \sin \theta, \quad (1)$$

vilket motsvarar signalens vägskillnad mellan intilliggande antenner. Således är den observerade fasförskjutningen mellan två intilliggande antenner

$$\varphi = \frac{2\pi d \sin \theta}{\lambda}. \quad (2)$$

Utifrån Ekvation 2 beräknas den infallande signalens vinkel enligt

$$\theta = \arcsin\left(\frac{\varphi \lambda}{2\pi d}\right). \quad (3)$$

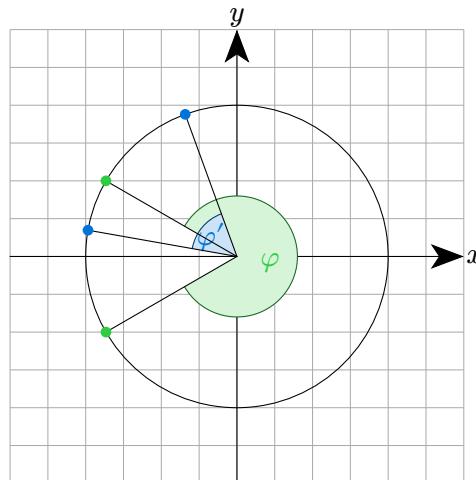
2.5 Channel state information

Fasforskjutningen kan härledas från data om signalförhållandena, så kallad *Channel State Information (CSI)*, som rapporteras kontinuerligt av wifikretsen för varje ansluten enhet. Från varje antenn fås en så kallad CSI-vektor med komplexa tal

$$A = \begin{pmatrix} a_1 e^{i\alpha_1} \\ a_2 e^{i\alpha_2} \\ a_3 e^{i\alpha_3} \\ \vdots \\ a_n e^{i\alpha_n} \end{pmatrix}, \quad B = \begin{pmatrix} b_1 e^{i\beta_1} \\ b_2 e^{i\beta_2} \\ b_3 e^{i\beta_3} \\ \vdots \\ b_n e^{i\beta_n} \end{pmatrix} \quad \text{respektive} \quad C = \begin{pmatrix} c_1 e^{i\gamma_1} \\ c_2 e^{i\gamma_2} \\ c_3 e^{i\gamma_3} \\ \vdots \\ c_n e^{i\gamma_n} \end{pmatrix} \quad (4)$$

där a_k , b_k och c_k är den k :te underbärarens signalstyrka och α_k , β_k , γ_k dess fas, för första, andra respektive tredje antennens. I följande stycket kommer vektorn A (som tillhör den första antennens) förklaras mer i detalj, men samma principer gäller även för de övriga antennernas CSI-vektorer.

Routerns maskinvara rapporterar de komplexa talen i rektangulär form (Gringoli m.fl., 2019) och således kan bara principalvärdet, som ligger i intervallet $(-\pi, \pi]$, erhållas för argumentet α_k .



Figur 6: Två olika par av faser (paren har var sin färg), förskjutna lika mycket från varandra, men som ger olika observerade fasforskjutningar.

Fasforskjutningen φ_k mellan två intilliggande antenner för den k :te underbäraren är differensen mellan motsvarande faser α_k och β_k , och ligger i intervallet $(-\pi, \pi)$. Uttrycket i Ekvation 3 har definitionsmängden $[-\frac{2\pi d}{\lambda}, \frac{2\pi d}{\lambda}]$ för φ och för att kunna beräkna ett entydigt värde på θ för alla vinklar mellan $-\pi$ och π måste därför $d \leq \lambda$. Med $d = \lambda$ är dock ett φ_k -värde nära ytterkanterna av värdemängden osannolikt, eftersom det förutsätter att de två faserna α_k och β_k också har värden nära ytterkanterna (-3 och 3 , till exempel; se Figur 6) – egentligen måste

$$d \leq \frac{\lambda}{2} \quad (5)$$

för att fasforskjutningarna $\varphi_1 \dots \varphi_n$ ska vara korrekta för alla $\theta \in (-\pi, \pi)$ – intervallet som är ekivalent med bredast möjliga ”synfält” för routern.

3 Metod

3.1 Materiel

Huvudkomponenten i lokaliseringssystemet är wifiroutern Asus RT-AC86U, som används eftersom dess wifikrets, Broadcom BCM4366, stödjs av CSI-extraheringsverktyget Nexmon framtaget av Gringoli m.fl. (2019). Dessutom har samma router använts i tidigare liknande experiment (Meneghelli m.fl., 2022; Pizarro m.fl., 2021; Schäfer m.fl., 2021). Dess antennavstånd d (se Figur 5 och Ekvation 3) är 0,09 m. I experimentet är antennerna inte riktade åt olika håll, som Figur 7 visar, utan samtliga är riktade rakt upp (de är vridbara).



Figur 7: Wifirouter märkt Asus RT-AC86U. De tre externa antennerna sitter på ovansidan. Routern har en fjärde intern antenn som inte används i experimentet.

3.2 Avgränsningar

De ekonomiska medlen tillgängliga för vårt förfogande kom från Norrnässtiftelsens stipendium vid summan ett tusen kronor. Nio hundra av dessa kronor användes vid inköp av en Asus RT-AC86U wifirouter genom Blocket. Wifiroutern Asus RT-AC86U kan bara mäta platta vinklar eftersom routerns antennsystem är endimensionellt samt ortogonal mot horisontalplanet (se Figur 5). Detta begränsar vår möjlighet att anlända vid en fullkomlig slutsats eftersom en wifienhets relation i höjd till routern inte går att mäta. Till exempel går det inte att avgöra från vilken våning av en byggnad en viss signal kommer.

Eftersom vi endast har en router att använda till experimentet är det inte heller möjligt att placera en avsändare genom dess vinklar mot en mängd andra mottagare eftersom triangulering kräver insamling av data från två eller fler mottagare. (Jämför Figur 8 med Figur 1.) I stället mäts precisionen av vinkeln mellan avsändaren och routern. Precisionen som uppnås genom detta visar på precisionen platsbestämning genom triangulering med två eller fler av dessa wifiroutrar skulle vara. En större budget – cirka två tusen kronor – hade behövts för att kunna använda två eller till och med tre identiska routrar till att genomföra triangulering.

På grund av ekonomiska begränsningar samt den stora mängd programmering nödvändig för ett fullständigt genomförande av detta experiment är det uppenbart att en mer omfattande investering krävts. Tid var i synnerhet begränsande.

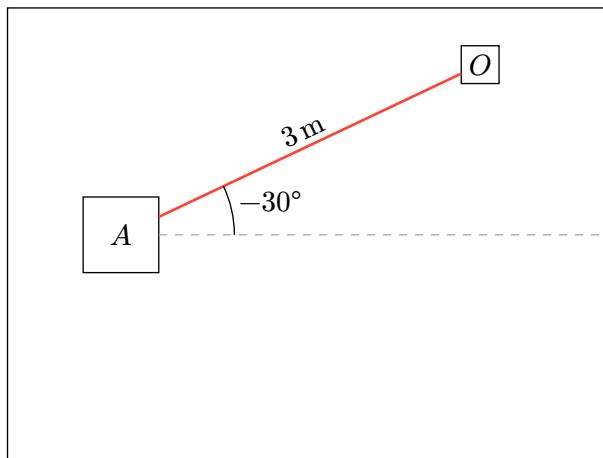
Med $d = 0,09\text{ m}$ och $\lambda = \frac{c}{5\text{ GHz}} \approx 6 \cdot 10^{-2}\text{ m}$ är olikheten i Ekvation 5 (som måste uppfyllas för att vinklar mellan -90° och 90° ska kunna mätas) falsk. Den uppenbara lösningen är att bygga om antennsystemet med förlängningskablar och ett mindre elementavstånd d , som Pizarro m.fl. (2021)

gjorde i sin studie med samma router, men vi saknade de ekonomiska medlen för att konstruera något liknande.

3.3 Genomförande

Genom att modifiera routerns maskinvara kan CSI erhållas (Gringoli m.fl., 2019): Programvarumodifikationsramverket Nexmon är testat med programvaruversion 10_10_122_20, så routerns programvara behövde nedgraderas. Därefter fördes `tcpdump`⁵ och Nexmons modifierade kernelmodul över till routern med SSH⁶.

Enheten placeras på ett bestämt avstånd från routern vid en bestämd vinkel enligt Figur 8.



Figur 8: Skiss (ovanifrån) över rummet som experimentet utfördes i med routern (*A*) och laptoppen (*O*). Routern är vänd med framsidan mot den streckade mittlinjen. Positiv vinkel innehåller att *O* är till höger om *A* (sett från routerns baksida); negativ vinkel betyder till vänster.

CSI-insamlingen görs genom att routern ställs in på samma kanal som enheten som ska spåras – i vårt fall styr vi över enheten och vilket wifinätverk den är ansluten till, och därmed känner vi till kanalen. Därefter genereras nätverkstrafik, vars CSI rapporteras av wifikretsen, med nätverkshastighetsmätverktyget Iperf⁷. På routern samlas *pcap-paket* från wifikretsen in (med programmet `tcpdump`) och skickas till en dator för analys.

Fält	Förklaring
Received signal strength indicator	Arbiträr signalstyrka
Avsändarens MAC-adress	Serienummer för avsändarens nätverksutrustning
Wifiramnummer	Unikt nummer för wifiramen ⁸ som gav upphov till detta CSI-fragment
Antennummer	Antennummer i intervallet [0, 3] (se Figur 7)
CSI	CSI-vektor (se Ekvation 4)

Tabell 3: Informationen som finns i ett pcap-paket från wifikretsen. (Gringoli m.fl., 2019)

⁵Enligt Nexmons anvisningar ska `tcpdump` användas till att samla in CSI. (Gringoli m.fl., 2019)

⁶SSH är ett lager 7-protokoll (precis som HTTP som beskrivs i Kapitel 2.2) som används för att säkert ansluta sig till andra nätverkshoteller.

⁷Iperf är ett program som används för att mäta nätverksprestanda genom att så mycket data som möjligt skickas mellan två nätverkshoteller (i vårt fall mellan enheten och en stationär dator på samma lokala nätverk). I experimentet konfigureras Iperf så att dataströmmen delas upp i så många wifiramar som möjligt, eftersom varje wifiram ger upphov till CSI.

⁸Det vill säga wifiramens ”kollinummer”.

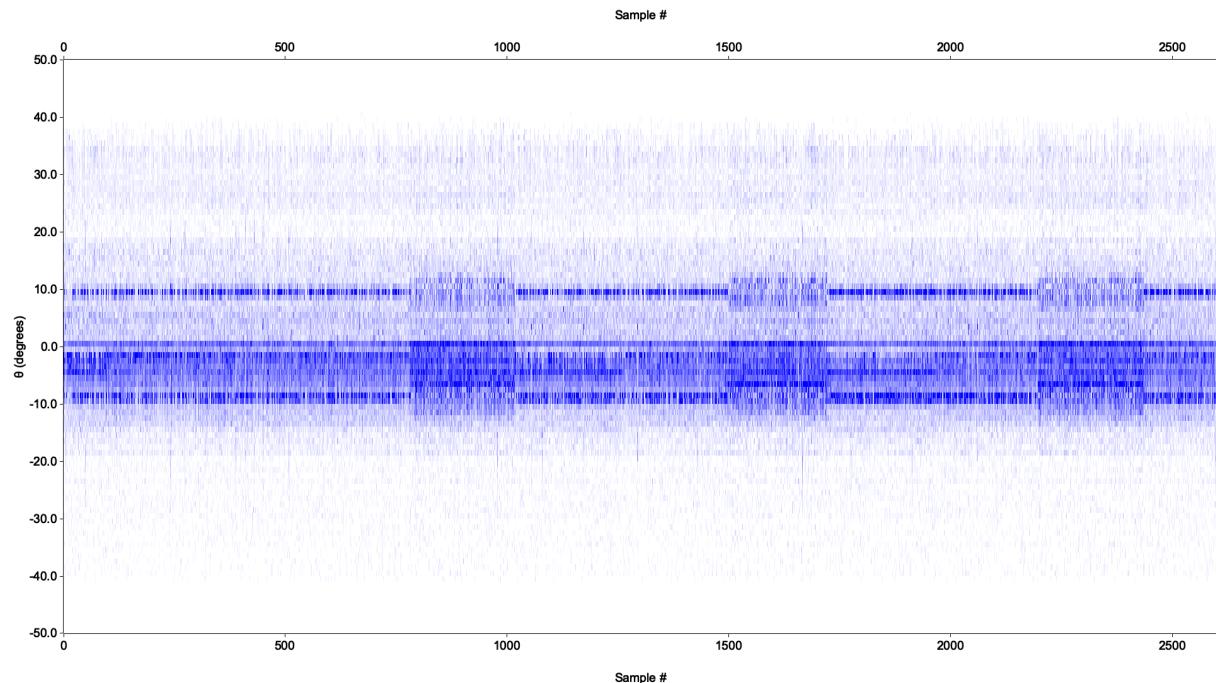
Ett pcap-paket genereras per antenn och wifiram och innehåller bland annat CSI (fullständig innehållsförteckning finns i Tabell 3), som filtreras beroende på MAC-adress (bara wifiramarna med enhetens MAC-adress sparas) och grupperas (i datorn) med andra pcap-paket utifrån ramnummer för att faserna från vektorerna A , B och C (Ekvation 4) ska kunna jämföras. Överensstämmande

Bestämningen av den infallande signalens vinkel (*Angle of Arrival, AoA*) görs enligt Ekvation 3 utifrån respektive fasförskjutning; dels mellan den mellersta och den högra antennen, dels mellan den vänstra och den högra antennen.

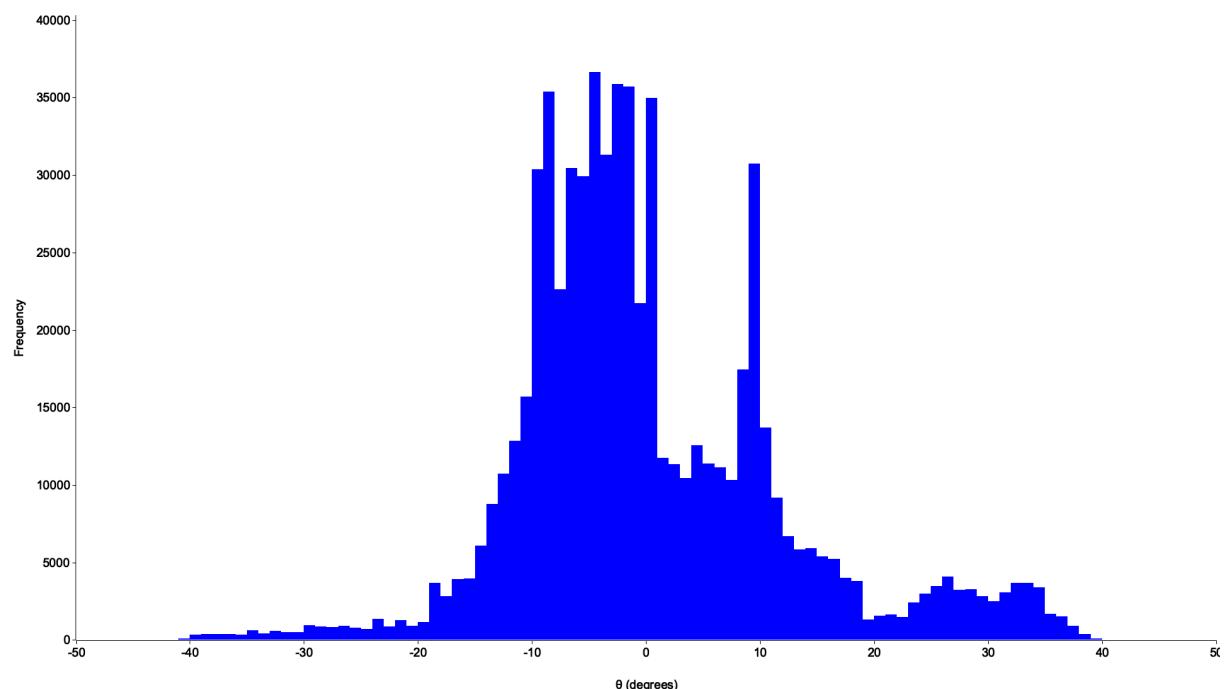
Samplingsfrekvensen för CSI är ungefär 230 Hz och AoA beräknas lika ofta. Experimentet genomförs för vinklarna $-30^\circ, -20^\circ, -10^\circ, \dots, 30^\circ$. AoA beräknas i cirka 10 s per vinkel.

4 Resultat och analys

På kanal 52, med bandbredden 40 MHz (vilket innebär att frekvenserna (5 250 till 5 290) MHz används), och med signalkällan ("enheten", en MacBook Air (2020)) 3,0 m från routern, avvek typvärdet för θ från det faktiska värdet, 0° , med som mest 10° under experimentet. Medelvärdet för θ under hela försöket var $0,2^\circ$ och standardavvikelsen var $11,9^\circ$.



Figur 9: Tvådimensionellt histogram över beräknad AoA för varje underbärare över tid. Vita områden har lägst frekvens⁹ (noll) och blå har högst.



Figur 10: Histogram över hur ofta varje θ beräknades, det vill säga summan av frekvenserna⁹ i Figur 9 tidvis (horisontellt i diagrammet).

⁹Frekvens som i förekomst – **inte** fysikalisk frekvens.

Diagrammen ovan visar detaljerad data för beräknad AoA då den verkliga vinkeln var 0° . Mätningarna upprepades för flera vinklar; resultatet återfinns i Tabell 4.

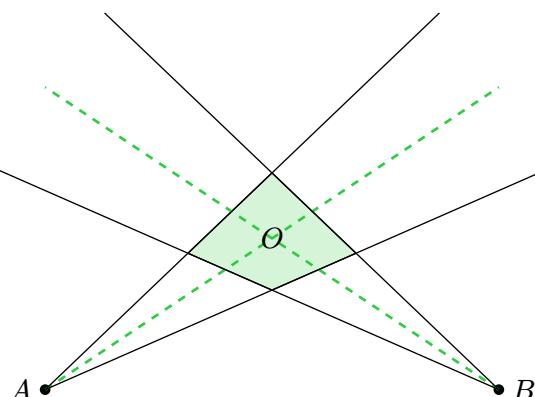
Faktisk vinkel	Avstånd till routern	$\bar{\theta}$	Avvikelse d	$\sigma_{\text{mätning}}$
-30°		$-31,2^\circ$	$1,2^\circ$	$13,2^\circ$
-20°		$-22,0^\circ$	$-2,0^\circ$	$10,3^\circ$
-10°		$-9,4^\circ$	$0,6^\circ$	$12,5^\circ$
0°	3,0 m	$0,2^\circ$	$0,2^\circ$	$11,9^\circ$
10°		$9,4^\circ$	$0,6^\circ$	$11,5^\circ$
20°		$20,2^\circ$	$0,2^\circ$	$10,9^\circ$
30°		$30,6^\circ$	$0,6^\circ$	$12,7^\circ$
Genomsnittlig avvikelse				$0,77^\circ$
σ_{total}				$0,59^\circ$

Tabell 4: Genomsnittliga uppmätta AoA $\bar{\theta}$ och standardavvikeler $\sigma_{\text{mätning}}$ för olika vinklar mellan routern och enheten (det vill säga standardavvikelsen av *samtliga* beräknade AoA; se Figur 10) samt den totala standardavvikelsen av alla avvikeler d , σ_{total} .

5 Diskussion

Ju närmare en wifienhet är till en router, desto högre precision i sträcka uppnås vid lokalisering av enheten rent geometriskt (se Figur 11). Eftersom platsbestämningen oftast kommer ske inomhus i närheten av en wifirouter innebär en felbedömning på $2,0^\circ$ endast ett fel på högst ett fåtal meter. Många rum i offentliga byggnader är redan utrustade med wifiroutrar¹⁰ och det skulle därför inte krävas en stor hårdvaruinvestering för att omprogrammera dem i statistiksyfte. Detta anser vi inte är helt orimligt ekonomiskt då det kunde utföras av två obetalda gymnasieelever inom loppet av ett par månader.

Precisionen som uppnåddes med wifiroutern Asus RT-AC86U är dock alldeles för låg för att denna metod ska kunna användas vid platsbestämning av wifiklienter utomhus. För att kompensera för en låg vinkelprecision krävs många wifiroutrar på en liten yta så att vinkelfelet inte leder till stora avståndsfel. Eftersom ytterst få wifiroutrar redan finns utomhus innebär detta att en mycket stor investering i hårdvara är nödvändig för att utvinna användbara resultat. Å andra sidan är sikten utomhus vanligen friare, vilket innebär färre störningselement för underbärarna och på så sätt att fler underbärare träffar antennsystemet direkt, utan att först reflekteras, och i det avseendet en högre precision.



Figur 11: Platsbestämning av O med hjälp av två routrar A och B i samma utförande som i detta experiment. Felmarginalen (här $(\pm 10)^\circ$) begränsar O :s position till en fyrhörning (ljusgrön i figuren).

Vid en första anblick är det inte konstigt att förvänta sig att alla underbärare ska nå antennerna från samma håll och därmed ge samma värde för θ . OFDM *förutsätter* i själva verket att de olika underbärarna tar olika väg, eftersom olika frekvenser fortplantas på olika vis vid reflektion och refraktion mot olika material, och så vidare, (se Kapitel 2.3) vilket visserligen går tvärt emot undersökningens syfte, men å andra sidan kan det användas till att analysera fysiska förhållanden i rummet. Schäfer m.fl. (2021) och He m.fl. (2020) använde till exempel CSI för att känna igen rörelsemönster hos människor enbart baserat på hur en wifisignals karaktär ändras när människorna i rummet rör sig.

Routern stod nära en vägg, i stället för fritt i rummet, vilket medförde höga risker för att signalen reflekterades mot väggen och *ytterligare* ökade antalet ”felriktade” underbärare. Detta minskar resultats validitet. Utöver detta undersöktes bara precisionen i en miljö samt med ett avstånd vilket vidare minskar resultats validitet.

6 Slutsats

Med wifiroutern Asus RT-AC86U går det att uppnå en precision där den genomsnittliga uppmätta AoA mellan routern och wifienheten avviker med som mest 2° från den faktiska vinkeln samt en medelavvikelse på $0,77^\circ$.

¹⁰Egentligen accesspunkter – bryggor mellan det trådbundna och det trådlösa nätverket. Det vedertagna uttrycket är dock *router*.

7 Bibliografi

- Gringoli, F., Schulz, M., Link, J., & Hollick, M. (2019). Free Your CSI: A Channel State Information Extraction Platform For Modern Wi-Fi Chipsets. *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*, 21–28. <https://doi.org/10.1145/3349623.3355477>
- He, Y., Chen, Y., Hu, Y., & Zeng, B. (2020). WiFi Vision: Sensing, Recognition, and Detection With Commodity MIMO-OFDM WiFi. *IEEE Internet of Things Journal*, 7(9), 8296–8317. <https://doi.org/10.1109/JIOT.2020.2989426>
- ISO Central Secretary. (1994). *Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model*. <https://www.iso.org/standard/20269.html>
- Lantmäteriet. *GPS – lantmateriet.se*.
- Meneghelli, F., Garlisi, D., Dal Fabbro, N., Tinnirello, I., & Rossi, M. (2022). *Wi-Fi channel frequency response database for contactless human activity recognition*.
- Phillips, G. (2023, december). *The most common Wi-Fi standards and types, explained*. <https://www.makeuseof.com/tag/understanding-common-wifi-standards-technology-explained/>
- Pizarro, A. B., Beltrán, J. P., Cominelli, M., Gringoli, F., & Widmer, J. (2021). Accurate Ubiquitous Localization with Off-the-Shelf IEEE 802.11ac Devices. *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, 241–254. <https://doi.org/10.1145/3458864.3468850>
- Schäfer, J., Barrsiwal, B. R., Kokhkhava, M., Adil, H., & Liebehenschel, J. (2021). Human Activity Recognition Using CSI Information with Nexmon. *Applied Sciences*, 11(19). <https://doi.org/10.3390/app11198860>
- Weinstein, S. B. (2009). The history of orthogonal frequency-division multiplexing [History of Communications]. *IEEE Communications Magazine*, 47(11), 26–35. <https://doi.org/10.1109/MCOM.2009.5307460>