UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Corso di Laurea Magistrale
in Ingegneria Informatica

Tesi di Laurea

Progettazione e realizzazione di un sistema di controllo flessibile del beamforming per apparati 802.11

Relatore: Prof. Francesco Gringoli
Correlatore: Dott. Marco Cominelli

Laureando:
Mauro Pozza
Matricola n. 708310

Anno Accademico 2020/21

Compendio

Con l'evoluzione degli standard Wi-Fi 802.11, sono state gradualmente introdotte una serie di funzionalità e ottimizzazioni con lo scopo di efficientare l'uso dello spettro elettromagnetico e migliorare la trasmissione di informazioni.
In questa tesi, è stata sviluppata una metodologia che permette all'utente di riconfigurare il *Beamforming*, una delle innovazioni inizialmente introdotte nello standard IEEE 802.11n, utilizzando esclusivamente dispositivi commerciali. Il sistema, permette infatti la completa costruzione di un *beamforming report*, ed il suo invio tramite un dispositivo in grado di operare come *Beamformee*, come un raspberry, un access point o ancora uno smartphone android, al fine di modificare il pattern di radiazione di un trasmettitore qualsiasi.
Il software utilizzato per la costruzione dei report è *Matlab*. Per attivare la trasmissione dei report iniettati dall'utente, è necessario modificare il firmware del beamformee, Per questo scopo, è stato utilizzato il framework *Nexmon* [20], in grado di gestire i chip radio usati in tutti i dispositivi testati. Non è invece necessaria alcuna modifica al dispositivo usato come trasmettitore, il quale accetta ed utilizza i report in arrivo come se fossero legittimi.

Indice

Capitolo 1

Introduzione

Il *Beamforming* esplicito è una tecnica presente negli standard Wi-Fi IEEE 802.11 a partire dalla versione n, che ha raggiunto la propria maturità con lo standard ac. Lo scopo principale di questa tecnologia, è quello di aumentare la potenza del segnale radio ricevuto in una particolare direzione, mantenendo la potenza globalmente emessa dal trasmettitore invariata, entro certi limiti imposti normativamente. Il modo con il quale questo risultato viene ottenuto è tramite lo sfasamento e la manipolazione del segnale in uscita da ciascuna antenna, posto che il trasmettitore sia dotato di almeno due antenne. Il motivo per il quale è richiesto un *Array* con almeno due antenne, è che la tecnologia in questione funziona grazie all'unione di più segnali trasmessi da sorgenti diverse, che si sommano costruttivamente lungo una direzione (*Beam*) prescelta, mentre non si influenzano o addirittura si sommano distruttivamente (abbattendo la potenza del segnale) altrove. Un effetto collaterale di questo comportamento è che il beamforming consente al dispositivo di trasmettere a più stazioni diverse e ben separate nello spazio circostante nello stesso lasso di tempo, focalizzando più beam indipendenti e privi di mutue interferenze verso la direzione di ciascun ricevitore. La configurazione del beamforming avviene in modo automatico tra i dispositivi impegnati dalla comunicazione, indipendentemente dalle scelte dell'utente finale. In questa tesi, sarà esposto il percorso seguito per implementare una versione del beamforming configurabile e gestibile da parte dell'utente utilizzando dispositivi commerciali. Per raggiungere questo fine, i primi capitoli si occuperanno di accompagnare il lettore lungo la folta giungla di modelli, standard e tecnologie necessarie a comprenderne il funzionamento. Successivamente, sarà presentato un capitolo dove viene descritto il software implementato per la gestione del beamforming ed infine, verranno presentati i dispositivi su cui è stato possibile testarlo con i relativi risultati ottenuti. La motivazione principale che ha spinto verso la creazione di questo sistema, è semplicemente di tipo sperimentale, in quanto al momento, al massimo delle nostre conoscenze, non è disponibile alcun framework per lo studio del beamforming

che non sia basato sull'adozione di SDR[1]. Queste radio, nonostante siano estremamente flessibili e permettano numerose configurazioni diverse, non sono di facile accesso per un utilizzatore finale, in quanto sono molto costose, implementano solamente il livello fisico dello standard, e comportano un notevole aumento di complessità nella loro gestione. Al contrario, il sistema sviluppato per questa tesi funziona su trasmettitori commerciali aderenti allo standard Wi-Fi 802.11. In questo modo, il problema del costo viene abbattuto, inoltre, il dispositivo in questione è già pienamente compatibile con le funzionalità previste dallo standard.
I campi di studio su cui la possibilità di controllare il beamforming può essere determinante sono molteplici, tra cui:

- L'uso della radiazione emessa non solo ai fini della comunicazione ma anche per studiare l'ambiente: stanno nascendo diversi algoritmi e metodi [7], [8] per poter localizzare e costruire la mappa di un ambiente chiuso (tipicamente l'interno di un edificio), dove le tecnologie gps e satellitare sono difficilmente adattabili e l'infrastruttura Wi-Fi è ampiamente adottata. La logica utilizzata per la mappatura dell'area circostante non necessita di fotocamere e non richiede l'accesso diretto a tutti i locali dell'ambiente, in quanto fa uso di una serie di antenne per misurare la dispersione delle onde radio contro la superficie. In casi come questo, poter concentrare la radiazione emessa verso direzioni precise permetterebbe di studiare la risposta del canale di comunicazione (CSI) nello specifico contesto selezionato dal trasmettitore, per poter mappare dettagliatamente diversi settori dell'ambiente.

- Lo studio delle CSI rappresenta un rischio alla privacy, in quanto permette a malintenzionati di controllare passivamente, attraverso tecniche di machine learning e fingerprinting, l'attivià e gli spostamenti di chiunque agisca all'interno dell'area di influenza della rete, anche di chi non è in possesso di alcun dispositivo Wi-Fi [22][23]. La survery [9], raccoglie ed analizza lo stato attuale dei lavori e delle tecniche principalmente utilizzate per questa attività, con i relativi pro e contro. Infatti, la sensibilità delle CSI è sufficientemente elevata da permettere di rilevare anche le minime perturbazioni allo stato iniziale dell'ambiente, come il movimento di una persona o l'aggiunta/la rimozione di un oggetto. Conoscendo quindi a priori le CSI ottenute in ambiente statico e le sue variazioni nel caso in cui ci sia presenza umana, è possibile classificare una nuova misurazione operando dei confronti con i dati precedentemente raccolti. In questo contesto, considerando che

[1]SDR - Software Defined Radio, sono delle implementazioni di sistemi di comunicazione radio dove i componenti fisici, caratterizzati da circuiti e dispositivi elettronici, sono in realtà implementati in un software in esecuzione su di un PC o più comunemente un sistema embedded dedicato.

variare la configurazione del beamforming implica una corrispondente variazione delle CSI misurate, è possibile invalidare a livello fisico la possibilità di studiare fingerprint dell'ambiente circostante, imponendo una variazione continua e casuale dello spettro delle CSI facendo sommare diversamente varie componenti spettrali e modificando la direzione del beam, modificando di conseguenza anche le misure ottenuta al dispositivo "spia" usato per la raccolta, pur mantenendo inalterata la comunicazione ed il normale scambio di dati. In ogni caso, influenzare le CSI con il beamforming non è l'unica soluzione per difendere la privacy da questi attacchi, ma vi sono altre tecniche di offuscazione e randomizzazione, come in [10] [11].

- Nelle operazioni Wi-FI, che per definizione avvengono liberamente nell'ambiente circostante, è fondamentale garantire l'autenticazione, la confidenzialità, e la sicurezza durante il trasferimento di dati, generando una coppia di chiavi condivise tra i soli due attori della comunicazione, che vengono usate per crittografare il flusso di informazioni scambiato. La tecnica più comune per la generazione di chiavi, prevede l'utilizzo di un terzo attore (certificate authority) e per questo è di difficile implementazione in ogni ambiente operativo. Di conseguenza, nel tempo sono stati studiati ed utilizzati algoritmi che permettono ai due attori della comunicazione di generare in modo autonomo e sicuro tutto il materiale crittografico. Fra gli altri, anche il famoso protocollo WPA fa parte di questa famiglia, ed è correntemente utilizzato nella sua versione *WPA2* per milioni di connessioni wifi casalinge e di tipo enterprise, tramite l'operazione di autenticazione a quattro vie (*4-ways-handshake*). Recentemente, tuttavia, è stato dimostrato come questa procedura presenti delle criticità a livello di sicurezza [12], richiedendo il passaggio ad una implementazione migliorata con WPA3, che fa uso della *Simultaneous Authentication of Equals (SAE)*. Per far fronte al continuo aumento di minacce nei confronti di questi protocolli di autenticazione, una delle strategie che sta recentemente venendo adottata per la generazione di chiavi è quella di utilizzare algoritmi che operano con il livello fisico della comunicazione [13]. Tra questi nuovi algoritmi, se ne evidenziano alcuni che sfruttano lo studio delle CSI [14] per migliorare la qualità delle chiavi scambiate, introducendo nello scambio delle quantità che sono visibili esclusivamente ai due attori della comunicazione. La sensibilità delle CSI, infatti, unita alla naturale variabilità dell'ambiente, rende sufficientemente improbabile ottenere più volte esattamente la stessa lettura, anche usando dispositivi molto vicini l'uno all'altro. Inoltre, le CSI misurate dal ricevitore e dal trasmettitore nello stesso istante hanno una fortissima correlazione, in quanto la radiazione emessa segue lo stesso percorso e subisce lo stesso tipo di dissolvenza per entrambi i sensi. Inserendo la capacità di controllare attivamente il beamforming in questo

contesto, è possibile modificare artificialmente le CSI misurate al ricevitore, aumentando il livello di casualità e correlazione rispetto a quanto ottenibile normalmente dai due attori.

Capitolo 2

Lo standard 802.11

2.1 Il modello OSI

Nel mondo delle telecomunicazioni, vista l'esigenza di standardizzare l'architettura logica con la quale diverse reti di calcolatori venivano progettate ed interconnesse, è nato, negli anni 80, il modello OSI (Open Systems Interconnection) in un formato aperto e non proprietario. L'ente che si è occupato della sua definizione è l'International Organization for Standardization (ISO), per questo motivo il modello è conosciuto anche con il termine *ISO/OSI*. Al suo interno non vi sono dettagli implementativi, in quanto è da intendersi come fonte concettuale sulla quale poi sviluppare delle implementazioni fisiche specifiche.

L'approccio con il quale l'ISO/OSI è stato pensato è un modello a strati, dove il problema della comunicazione tra due o più entità viene suddiviso in più sottoproblemi tramite la metodologia del *divide et impera*, grazie alla quale ogni aspetto (livello) può essere gestito in completa autonomia rispetto agli altri, garantendo così modularità ed intercambiabilità. Per permettere questa stratificazione, i servizi e l'interfaccia che un determinato livello deve offrire al livello superiore sono definiti dal modello, e sono quindi indipendenti dall'implementazione .

Il numero di livelli previsto dall'ISO/OSI è pari a sette (figura 2.1). La scelta del numero e del tipo di livelli è cruciale per garantire che una specifica funzione non sia separata in più livelli e che non ci siano funzionalità ridondate (dovute per esempio alla presenza di troppi livelli). La conseguenza di una struttura di questo tipo è che se i primi livelli - Fisico, Collegamento dati e Rete - dipendono rispettivamente dal mezzo fisico (wireless, rame, fibra), dal tipo di connessione tra due nodi e dall'infrastruttura di rete, più ci si sposta a livelli superiori più ci si astrae dall'implementazione fisica, per dedicarsi alla gestione applicativa e alla

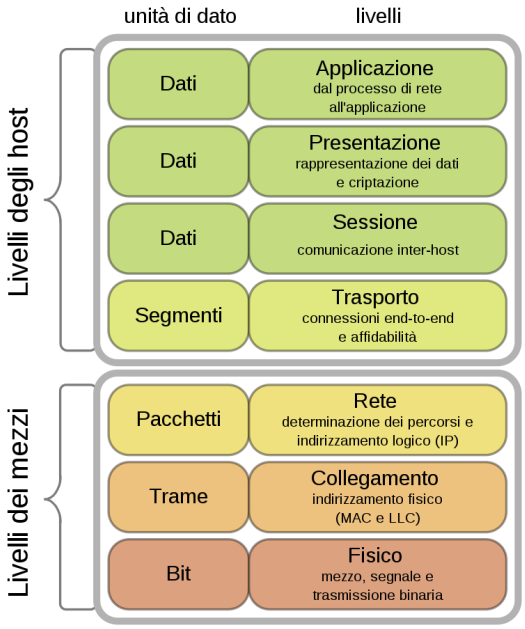

Figura 2.1: Stack del modello OSI. I livelli sono ordinati a partire dal basso verso l'alto.

fornitura di servizi all'utente. Per gli aspetti che verranno trattati in questa tesi, sarà sufficiente espandere i primi due livelli del modello.

Livello Fisico Come preannunciato, il primo livello dello standard ISO/OSI è il livello fisico, che è direttamente associato alla connessione che materialmente congiunge due o più dispositivi. Il tipo di dato che viene trattato e trasmesso a questo livello è l'unità informativa elementare nell'informatica: il singolo bit, il quale rappresenta uno stato logico che può assumere due valori, tipicamente indicati con "1" e "0". In realtà, a seconda della convenzione e della tecnologia utilizzata, uno stream di più bit può essere raggruppato in un "simbolo" o "parola", che saranno il tipo di dato atomico usato nella comunicazione.
Vista la natura del livello in questione, è necessario che siano fornite anche tutte le specifiche relative al mezzo di comunicazione, come la descrizione meccanica dei connettori elettrici in uso, la tipologia di cavo (se previsto) con la lunghezza massima e la relativa impedenza, le frequenze utilizzate, la potenza dei segnali. Inoltre, il livello fisico deve occuparsi della sincronizzazione tra il trasmettitore ed il ricevitore durante la trasmissione, e sono introdotte tecniche di equalizzazione e correzione degli errori per aumentare l'efficienza.
Tutti questi aspetti, sono tipicamente gestiti da un circuito elettronico dedicato,

che viene chiamato *PHY*. Nel caso dello standard 802.11 per il Wi-Fi, il chip che si occupa della comunicazione deve contenere anche un ricevitore radio, con amplificatori, filtri, un'interfaccia verso l'antenna, convertitori analogico-digitali e un micro-controllore o un'unità di elaborazione per l'esecuzione delle istruzioni relative alla comunicazione.

Livello di collegamento dati Questo livello fornisce i mezzi per gestire il trasferimento di trame (frames) tra i dispositivi connessi dal livello fisico. All'interno del frame sono indicati gli indirizzi usati per identificare il dispositivo sorgente ed il dispositivo destinatario della comunicazione.
I servizi offerti sono:

- Sincronizzazione dei frame: viene determinato l'inizio e la fine di un frame per permetterne la ricostruzione al ricevitore, partendo dal flusso di bit.
- Controllo del flusso: Viene gestita la velocità di comunicazione per massimizzare il trasporto di dati senza che il ricevitore venga saturato
- Controllo degli errori, anche se alcune implementazioni ne sono prive e ne lasciano la gestione ai livelli superiori
- Gestione degli accessi multipli: cruciale quando ci sono più dispositivi connessi alla rete fisica, serve per evitare che due trasmissioni separate si incontrino causando interferenza distruttiva. Tra i protocolli più conosciuti in questo ambito vi è il CSMA *Carrier Sense Multiple Access* nelle sue versioni CSMA/CD (*Collision Detection - Rilevamento delle collisioni*), utilizzato nella rete Ethernet, e CSMA/CD (*Collision Avoidance - Evitamento delle collusioni*) utilizzato nelle reti Wi-Fi.

Nella realtà dei fatti, lo standard ISO/OSI è utilizzato più come un riferimento sul quale basare la propria architettura anziché un modello rigido. Infatti, nonostante la quasi totalità delle implementazioni reali di protocolli rete segua lo stesso approccio a strati, è comune che il numero di livelli e le funzionalità offerte da ciascuno di essi sia diverso da quanto stabilito dall'ISO. L'esempio più notevole riguarda l'architettura TCP/IP[1], che fornisce tutto l'insieme di protocolli su cui si basa l'internet. Originariamente, il TCP/IP non era strutturato in una serie gerarchica di livelli, in quanto era nato con un approccio più pragmatico, nell'intento di formulare una suite di protocolli funzionante e facilmente implementabile, prima che se ne fosse potuto analizzare l'aspetto teorico e formale. In seguito alla

[1]Il nome TCP/IP è mutuato dal nome di due dei protocolli più famosi che ne fanno parte: l'IP (Internet Protocol), che gestisce il livello di rete e il TCP (Transmission Control Protocol), che gestisce il livello di trasporto.

sua definizione, che è avvenuta prima dell'avvento dell'ISO/OSI, si è tentato di ricavarne un modello basato su quattro livelli, che in figura 2.2 sono paragonati all'ISO/OSI. Le differenze sostanziali sono relative al livello applicativo, che nel caso del TCP/IP ingloba anche i servizi dei livelli 5, 6 e 7 del modello OSI.

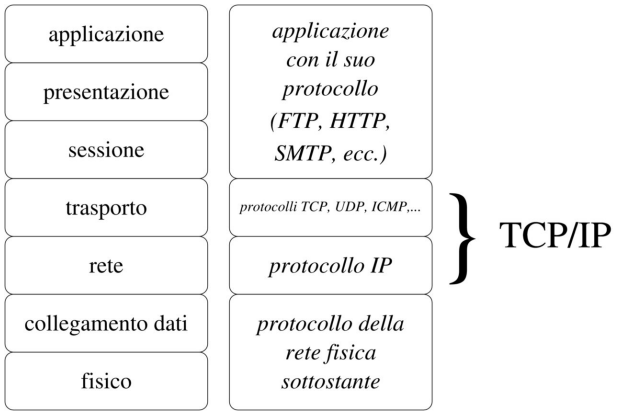

Figura 2.2: Confronto tra il modello ISO/OSI e l'architettura TCP/IP.

2.2 La commissione IEEE 802 LAN/MAN

Gli standard IEEE 802[2], gestiti dall' *Institute of Electrical and Electronics Engineers*, sono una serie di standard preposti alla gestione di tutte le specifiche di reti LAN di calcolatori che hanno pacchetti a lunghezza variabile. A differenza del modello ISO/OSI, l'IEEE 802 non fornisce delle specifiche astratte, ma per ciascuno standard definisce le caratteristiche tecniche necessarie per potervi aderire.

La struttura definita dallo standard IEEE 802 è composta da tre livelli (figura 2.3), che occupano lo spazio identificato dai primi due livelli del modello ISO/OSI. Il primo livello fisico *(PHY)*, definisce le proprietà fisiche del mezzo di comunicazione. Il secondo livello *MAC, Medium Access Control* si occupa di gestire la comunicazione con il mezzo fisico ed il terzo livello *LLC, Logical Link Control*, specificato nello standard IEEE 802.2, funge da interfaccia tra i livelli MAC inferiori e il livello di rete.

[2]Il numero 802 non ha alcun significato: era semplicemente il primo numero libero negli standard IEEE al momento della formazione del comitato che se ne è occupato per la prima volta

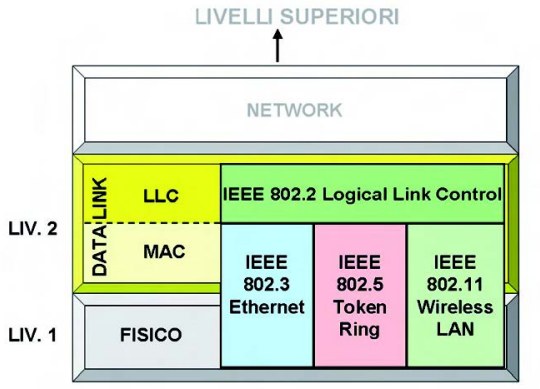

Figura 2.3: Gli standard IEEE 802 nello stack OSI

Vista la forte dipendenza del *MAC* con il livello fisico, è stato introdotto per i primi due livelli uno standard diverso e specifico per ciascun mezzo di comunicazione. Nell'esempio mostrato in figura 2.3, si possono vedere lo standard 802.3 Ethernet (la rete cablata più diffusa, gestita tipicamente con connessioni in rame o in fibra ottica), lo standard 802.5 Token Ring (una particolare rete cablata introdotta da IBM nel 1984) e lo standard 802.11 Wireless (per le reti LAN Wi-Fi senza cavi). La presenza in contemporanea del più noto standard per reti LAN cablate e del più noto standard per reti Wi-Fi, rende la conoscenza della famiglia IEEE 802 un aspetto fondamentale nell'ambito della gestione di reti e di infrastrutture di rete. Per garantire una interoperabilità tra tutti gli standard, dal livello LLC in poi, ogni frame, indipendentemente dallo standard utilizzato, viene ricostruito secondo le regole dello standard 802.3 e trattato da tutti i livelli superiori come tale.

2.3 Lo standard IEEE 802.11

2.3.1 Mezzo fisico

Il mezzo di comunicazione utilizzato dagli apparati Wi-Fi compatibili con lo standard 802.11 è l'onda elettromagnetica alle frequenze limitate dallo spettro radio (3hz - 3000Ghz). Questo tipo di onda non ha bisogno di alcun mezzo materiale per poter viaggiare nello spazio, in quanto è il frutto della propagazione di campi elettromagnetici, i quali si "muovono" con una velocità vicino a quella della luce[3]. La generazione di questi campi elettromagnetici avviene all'interno dell'antenna

[3]Velocità della luce nel vuoto: $C \simeq 3 * 10^8\ m/s$, La velocità reale è leggermente inferiore a causa della presenza dell'atmosfera terrestre

del trasmettitore, applicandovi un segnale elettrico che genera un flusso di elettroni (per questo motivo l'antenna deve essere di un materiale conduttore). Allo stesso modo, nell'antenna usata come ricevitore, il campo elettromagnetico proveniente dal trasmettitore provoca a sua volta un'oscillazione di elettroni, che viene utilizzata per leggere l'informazione trasmessa. L'obiettivo di questo sistema di comunicazione è recuperare in ricezione un segnale con forma d'onda uguale (o più simile possibile) a quella di partenza.

Caratteristiche delle onde elettromagnetiche

In questo breve paragrafo sono introdotte le caratteristiche dei segnali elettromagnetiche (con riferimento alla figura 2.4) utili ai fini della lettura di questa tesi.

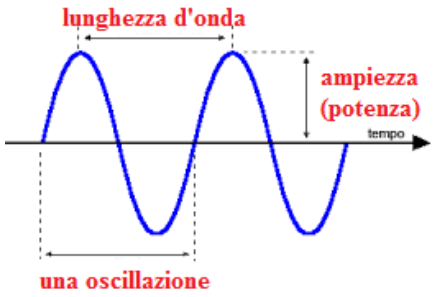

Figura 2.4: Segnale sinusoidale

- L'onda elettromagnetica è interpretata come un segnale: una funzione matematica del tempo. Questo segnale può essere rappresentato come una somma di sinusoidi.
- La rappresentazione della funzione data da un segnale sinusoidale è: $A\cos(\omega_0 t + \phi_0)$.
- Pulsazione: ω_0. Si misura in rad/s. $\omega_0 = 2\pi f_0$
- Frequenza f_0: Numero di cicli della forma d'onda ripetuti al secondo. Si misura in hertz (Hz)
- Periodo T: $1/f$
- Lunghezza d'onda λ: Distanza tra due *creste* dell'onda. Si misura in metri.
- Ampiezza: differenza tra il valore massimo dell'onda ed il valore di equilibrio (0).

- Rapporto inverso tra frequenza e lunghezza d'onda: $\lambda = \frac{v}{f}$. con v velocità di propagazione ($\simeq 3 * 10^8\ m/s$).
  Se $f = 2.4ghz => \lambda = 12.5cm$

- fase iniziale ϕ_0: rappresenta la traslazione orizzontale di una sinusoide rispetto a un'altra, presa come riferimento

- Le onde elettromagnetiche sono in grado di penetrare superfici. Onde con una frequenza più alta hanno una capacità di penetrazione inferiore.

- All'aumentare della lunghezza d'onda (e quindi al diminuire della frequenza) aumenta la capacità di propagazione nello spazio del segnale.
  La relazione nello specifico è la seguente: con l'aumentare della distanza dalla sorgente, la perdita di potenza di trasmissione è pari al quadrato della frequenza del segnale.

- All'aumentare della lunghezza d'onda aumenta anche la dimensione che deve avere l'antenna.

Le frequenze usate dagli standard 802.11 sono il frutto di questi compromessi: si è scelta una frequenza abbastanza bassa da avere un range ideale, e nel contempo abbastanza alta da permettere l'integrazione di antenne in dispositivi portatili.

Gestione dello spettro

Per evitare interferenze durante tutte le possibili fasi di comunicazione radio, lo spettro disponibile è rigorosamente controllato e gestito da una serie di autorità tecniche/governative. Nel caso dell'europa si tratta della *CEPT (Conferenza Europea delle amministrazioni delle Poste e delle Telecomunicazioni)*, tramite l'*ERO (European Radiocommunication Office)*, ma più in generale a livello internazionale tramite l'*ITU (International Telecommunications Union)*. La maggior parte dello spettro disponibile viene rilasciato solo tramite licenza, ed è dedicato a specifici utilizzi (per esempio le frequenze nella banda 87,5 - 108 Mhz sono riservate alla radio FM). Tuttavia, ci sono alcune bande (tabella 2.1) definite *ISM* (Per scopi Industriali, Medici e Scientifici) in cui su parte delle frequenze, pur imponendo una serie di limitazioni, è permessa la libera emissione nello spettro ai dispositivi certificati. Questa loro caratteristica ha reso le bande ISM molto popolari: nella fattispecie, gli apparecchi wireless 802.11 utilizzano principalmente le frequenze centrate a 2450Mhz - perciò, il Wi-Fi a queste frequenze si chiama anche 2.4 GHz. Altri utilizzi comuni della banda 2.4 GHz sono le frequenze usate dal forno a mi-

croonde[4] ed il bluetooth. Con l'introduzione dello standard 802.11a nel 1999 si è aperta la strada ad un'altra banda chiamata *U-UNII (Unlicensed National Information Infrastructure)* che opera nell'intorno dei 5 Ghz. Proprio grazie alla libertà concessa nelle frequenze ISM e U-UNII è possibile installare un router Wi-Fi in un appartamento o un ufficio senza debba chiedere alcuna certificazione per l'emissione in quel particolare campo[5]. Soprattutto per quanto riguarda la frequenza 2.4 Ghz, la sua enorme popolarità porta con sè anche un lato negativo: vi è una costante emissione di onde nello spettro usato dallo standard 802.11, che genera interferenze e rumori i quali rendono la trasmissione di un dato senza perdite in questa frequenza più difficile.

Intervallo di Frequenza	Larghezza di banda	Frequenza Centrale
6.765 - 6.975 Mhz	0.03 MHz	6.78 MHz
13.553 - 13.567 Mhz	0.014 MHz	13.56 MHz
26.957 - 27.283 Mhz	0.326 MHz	27.18 MHz
40.66 - 40.7 Mhz	0.04 MHz	40.68 MHz
433.05 - 434.79 Mhz	1.74 MHz	433.92 MHz
902 - 928 Mhz	26 MHz	915 MHz
2400 - 2500 Mhz	100 MHz	2450 MHz
5725 - 5875 Mhz	150 MHz	5800 MHz
24 - 24.250 Ghz	250 MHz	24.125 GHz
61 - 61.5 Ghz	500 MHz	61.250 GHz
122 - 123 Ghz	1000 MHz	122.5 GHz
244 - 246 Ghz	2000 MHz	245 GHz

Tabella 2.1: Lista delle frequenze ISM

PHY

Il livello fisico (*PHY*) specificato nello standard 802.11, si occupa di definire le specifiche fisiche ed elettriche dei dispositivi. Le sue funzioni principali sono quelle di stabilire e terminare una connessione tra i mezzi di comunicazione e convertire i dati dalla rappresentazione digitale propria del dispositivo in uso alla corrispondente modulazione analogica del segnale. Per lo svolgimento di questi compiti sono stati introdotti due sottolivelli (visibili in figura 2.5), più un livello di gestione.

[4]Le potenze emesse da un forno a microonde sono ordini di grandezza superiori a quanto permesso per un'antenna Wi-Fi, che quindi non è minimamente in grado di provocare gli stessi effetti di riscaldamento.

[5]Come già detto però, il dispositivo utilizzato deve essere comunque certificato allo standard. La certificazione non viene fornita direttamente dall'IEEE ma da un ente non-profit creato appositamente per lo scopo, chiamato *Wi-Fi Alliance*.

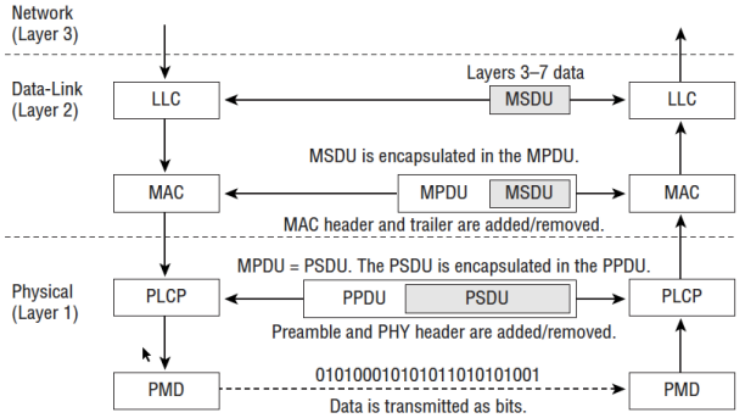

Figura 2.5: Dettaglio dell'architettura 802.11

Il primo livello *PLCP (Physical Layer Convergence Protocol)* riceve dal MAC un *MPDU (MAC protocol data units)*[6] contenente il messaggio da inviare incapsulato con tutte le informazioni necessarie alla comunicazione aggiunte dai livelli superiori. La sua funzione è quella di generare un frame che abbia un formato compatibile con la trasmissione effettuata dal PMD.
Il *PMD (Physical Medium Dependent)* si occupa di eseguire la vera e propria trasmissione, in questo caso tramite onde elettromagnetiche.

Lo standard 802.11 è in continua evoluzione nel tempo, e prevede il rilascio di nuove versioni che ne cambiano il funzionamento e le tecniche di trasmissione. In figura 2.6 sono mostrate in ordine le generazioni più popolari che sono state rilasciate, la loro velocità massima teorica, l'anno di standardizzazione e le frequenze utilizzate[7]. Nei paragrafi seguenti verrà presentato più in dettaglio lo standard 802.11ac per due motivi principali:

- Insieme al più vecchio 802.11n è lo standard più utilizzato (il Wi-Fi 6 è stato introdotto solo recentemente e sopratutto in ambito casalingo deve ancora guadagnare quote di mercato).
- È lo standard principalmente utilizzato durante le fasi di laboratorio per il controllo del Beamforming.

[6] L'MPDU viene anche chiamato *PSDU (PLCP Service Data Unit)*

[7] La nomenclatura Wi-Fi 4-6 incrementale è stata introdotta successivamente al rilascio dello standard 802.11ac, e applicata retroattivamente alle due versione precedenti. I termini Wi-Fi 1-3 sono perciò non ufficiali. Prima di questa denominazione, si utilizzava come riferimento il solo nome dello standard

Wi-Fi generations			
Generation/IEEE Standard	**Maximum Linkrate**	**Adopted**	**Frequency**
Wi-Fi 6 (802.11ax)	600–9608 Mbit/s	2019	2.4/5 GHz 1–6 GHz ISM
Wi-Fi 5 (802.11ac)	433–6933 Mbit/s	2014	5 GHz
Wi-Fi 4 (802.11n)	72–600 Mbit/s	2009	2.4/5 GHz
Wi-Fi 3 (802.11g)	3–54 Mbit/s	2003	2.4 GHz
Wi-Fi 2 (802.11a)	1.5 to 54 Mbit/s	1999	5 GHz
Wi-Fi 1 (802.11b)	1 to 11 Mbit/s	1999	2.4 GHz

Figura 2.6: Generazioni Wi-Fi

La prima versione dello standard (chiamata *Legacy*) non è mostrata in figura. È stata rilasciata nel 1997, aveva una velocità di trasmissione pari a 1/2 Mbps ed introduceva tre livelli fisici differenti, chiamati DSSS, FHSS e una versione ad infrarossi, che non sono più attualmente in uso in alcuna versione.

Lo standard 802.11a è stato il primo ad utilizzare la banda 5Ghz e ad introdurre l'OFDM al livello fisico, che è stato poi utilizzato come base per tutti i successivi standard. Nonostante ciò, l'802.11a non ha goduto di una grande distribuzione perché è stato commercialmente sconfitto dal più economico e tradizionale 802.11b, rilasciato lo stesso anno.

Capitolo 3

Lo standard IEEE 802.11ac

Lo standard 802.11AC è stato introdotto nel 2013, come un miglioramento rispetto a quanto implementato nel precedente standard 802.11n del 2006. Le principali novità che verranno analizzate in questa tesi sono l'uso di canali più ampi, l'uso esclusivo della frequenza a 5Ghz, abbandonando di fatto i 2.4Ghz, la semplificazione della modulazione e del beamforming, l'introduzione di una modulazione più aggressiva, l'introduzione del MU-MIMO (MultiUser MIMO) e l'introduzione del supporto ad array fino ad otto antenne attive in parallelo.

3.1 Canali utilizzati

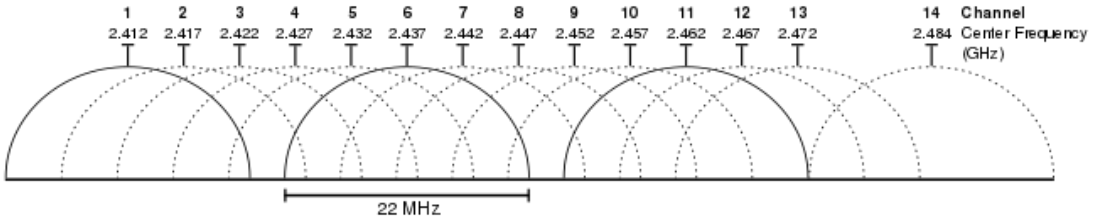

Figura 3.1: Canali Wi-Fi nella banda 2.4Ghz

Per permettere la comunicazione tra più stazioni all'interno delle frequenze utilizzate, l'ampio spettro elettromagnetico a disposizione sia nel caso dei 2.4Ghz che dei 5Ghz viene suddiviso in canali a cui ciascuna trasmissione deve limitarsi. In figura 3.1 è presentata la suddivisione della banda 2.4Ghz in 14 canali, ciascuno con una ampiezza di 20Mhz, a cui vanno aggiunti 2Mhz di guardia per permettere l'attenuazione ai confini del canale. Quando due terminali stanno per avviare una comunicazione, dovranno scegliere uno dei canali possibili, identificati dalla

frequenza centrale, tipicamente preferendo canali sui quali misurano un numero di interferenze inferiore. Come risulta evidente, la maggior parte dei canali è sovrapposta ad altri, e l'unica combinazione priva di sovrapposizioni prevede l'uso dei soli canali 1, 6 e 11 (più il 14 dove previsto dalle regolazioni vigenti). L'utilizzo di canali sovrapposti è comunque possibile, anche se aumenta il rischio di interferenze e quindi richiede che vengano impiegati degli schemi di modulazione più conservativi, rallentando così la velocità di comunicazione. In ogni caso, considerato l'elevato numero di dispositivi Wi-Fi in circolazione, normalmente ci si ritrova comunque ad avere più trasmissioni in concorrenza sullo stesso canale.

Adottando la modulazione OFDM, anche la forma dei canali cambia (figura 3.2) rispetto a quanto visto in figura 3.1. Il modo con il quale si ottiene questa particolare forma dipende dalle limitazioni che lo standard impone alla potenza emessa sul canale, man mano che ci si allontana dalla frequenza centrale. Nello specifico, sono introdotte quattro limitazioni diverse: fino a 9 Mhz di distanza dalla frequenza centrale è ammessa la potenza massima, da 9 a 11 mhz di distanza si impone una limitazione di -20dBr[1] rispetto alla potenza massima, da 11 a 20 mhz si scende a -28dBr e oltre i 30 mhz si arriva a -40dBr. Grazie a questo comportamento ci si assicura che alle estremità il segnale sia abbastanza attenuato da non causare interferenze rilevante nei canali adiacenti.

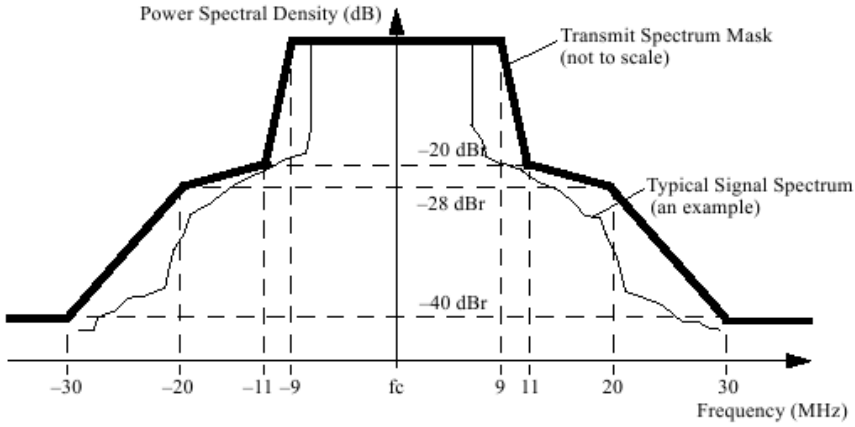

Figura 3.2: Maschera spettrale di un canale OFDM da 20Mhz

In figura 3.3 sono mostrati i canali OFDM a 5Ghz che sono stati resi disponibili per la comunicazione Wi-Fi in Europa. La quantità di canali a disposizione nel

[1]La sigla dBr significa *Decibels relative to reference level - Decibel relativi al livello di riferimento*

mondo non è fissa ma è soggetta a differenzi regolazioni (inter)nazionali, che ne decidono la quota utilizzabile. Osservando la figura, è possibile notare come non sia prevista la sola presenza di canali a 20 Mhz: a partire dall'802.11n sono stati introdotti canali con un'ampiezza pari a 40 Mhz e con l'avvento dell'802.11ac sono stati inseriti anche canali a 80 e a 160 Mhz. Per ottenere un Canale a 80 Mhz, è necessario aggregare due canali adiacenti da 40 Mhz, che a loro volta devono aggregare due canali adiacenti da 20 Mhz, per un totale di quattro canali da 20 Mhz tutti adiacenti l'uno con l'altro. Se operazioni di questo tipo sono possibili nelle frequenze a 5 Ghz, lo stesso non si può dire per i 2.4 Ghz, dove, avendo a disposizione una banda complessiva di 100 Mhz, implementare un canale di 80Mhz equivarrebbe ad occupare quasi tutti i canali utilizzabili.
Considerando i vincoli di aggregazione di canali da 20Mhz per poter trasmettere su ampiezze maggiori (come 40 o 80Mhz), e considerando il fatto che una coppia trasmettitore-ricevitore è libera di cambiare dinamicamente l'ampiezza del canale in uso durante la trasmissione in base alle proprie esigenze, anche la gestione dei canali nella banda a 5Ghz implica una serie di accortezze per ottimizzarne l'uso. Per esempio, ipotizzando uno scenario nel quale due trasmettitori diversi abbiano inizialmente occupato due canali da 20mhz adiacenti, nel caso in cui uno di questi avesse la necessità di muoversi su un canale da 40mhz, la presenza dell'altra trasmissione sul canale adiacente impedirebbe di fatto l'acquisizione delle frequenze necessarie senza causare interferenze, e relegherebbe entrambi i trasmettitori ai soli canali di ampiezza minore. È così previsto che, nei limiti del possibile, i canali scelti per la trasmissione siano sufficientemente distanti l'uno dall'altro da permettere alle stazioni adiacenti di muoversi verso canali ad ampiezze superiori senza ritrovarsi uno dei canali 20mhz da aggregare già saturato da altre comunicazioni.

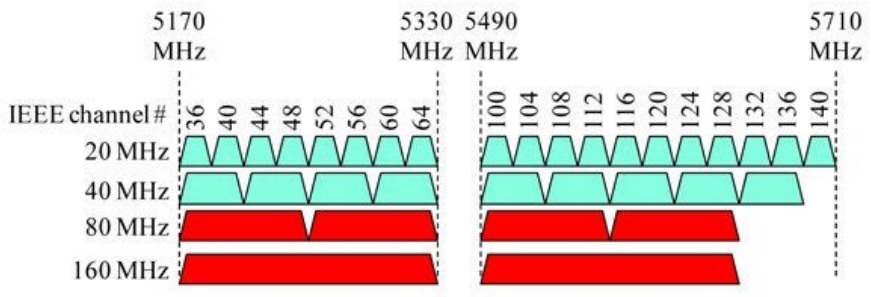

Figura 3.3: Canali Wi-Fi nella banda 5Ghz disponibili in Europa

Nota: Le attenuazioni imposte dalla modulazione OFDM per un canale da 20 Mhz viste in figura 3.2, si mantengono valide anche per canali di ampiezza supe-

riore, modificando le distanze soglia dalla frequenza centrale per poter preservare la stessa maschera spettrale sulla frequenza maggiore.

3.2 La trasmissione Orthogonal Frequency Division Multiplexing

L'OFDM (Orthogonal Frequency Division Multiplexing) è una tecnica di trasmissione digitale in uso nell'802.11ac, introdotta da Robert W. Chang nel 1966 ed utilizzata per la prima volta nelle comunicazioni Wi-Fi dallo standard IEEE 802.11a. La sua caratteristica principale è quella di dividere la trasmissione all'interno di un singolo canale in più sotto-canali (nello standard 802.11ac per un canale da 20 Mhz sono 64, ciascuno con un'ampiezza pari a 312.5 Khz), che vengono usati nella comunicazione in parallelo come se fossero dei canali distinti.

Per via dei limiti di potenza assunti da un canale OFDM da 20 Mhz (visti in figura 3.2), i sotto-canali usati per la comunicazione sono nell'intervallo [-28,28], in quanto al di fuori di questi valori l'attenuazione imposta risulta essere troppo elevata per una trasmissione efficace. Rimuovendo anche il sotto-canale centrale (0), dei 64 sotto-canali a disposizione solo 56 sono utilizzabili per la comunicazione, ai quali vanno rimossi altri quattro canali (-21, -7, 7 e 21) chiamati *pilota* che vengono utilizzati per funzioni di monitoraggio.

Il vantaggio dell'OFDM sta nel fatto che nonostante i sotto-canali siano sovrapposti l'uno con l'altro, non si verificano interferenze durante la comunicazione grazie alla proprietà dell'ortogonalità, che permette di distinguere e separare facilmente ciascun segnale eliminando il cross talk. Nella figura 3.4 si può notare come, per via di questa proprietà, in corrispondenza del picco di ciascun sotto-canale tutti gli altri abbiano un'ampiezza pari a zero.
L'abbattimento delle interferenze consente anche di semplificare la trasmissione in quanto non è necessario né utilizzare una banda di guardia tra un canale e l'altro nè alcun complesso filtro di equalizzazione. D'altro canto, è fondamentale che durante la comunicazione, la sincronizzazione in frequenza tra il trasmettitore ed il ricevitore sia precisissima, dato che anche una minima variazione risulterebbe essere problematica considerando la ridotta ampiezza di ciascum canale, con il rischio di perdere l'ortogonalità e ottenere così l'effetto dell'*Inter Carrier Interference (ICI)* - Interferenza tra sotto-canali.

Uno degli aspetti positivi nell'utilizzare più sotto-canali in parallelo per la comunicazione, è che ciascuno di essi può essere trattato come se fosse un canale

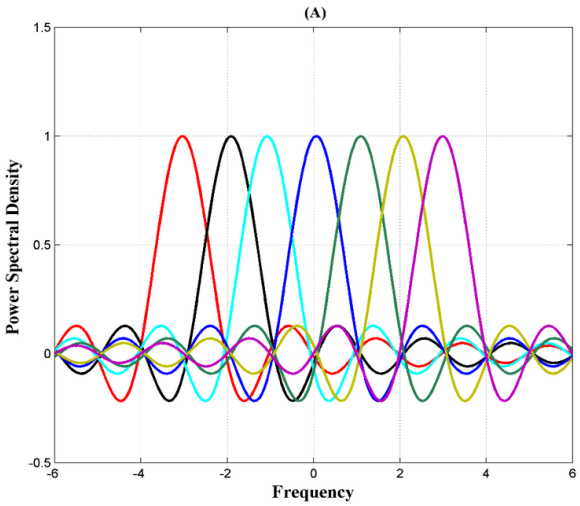

Figura 3.4: Ortogonalità di 7 canali OFDM

a se stante, con la propria modulazione. Inoltre, per abbattere ulteriormente le interferenze, è possibile utilizzare degli schemi di modulazione più conservativi, in quanto la quantità di informazione trasmissibile sommando tutti i sotto-canali risulta comunque essere superiore a quanto si potrebbe ottenere utilizzando tutto il singolo canale con modulazioni più aggressive. L'uso di una modulazione conservativa, implica la trasmissione di un numero inferiore di informazioni (di bit) per unità di tempo. La quota di tempo risparmiata, consente l'introduzione di un intervallo di guardia (posto all'inizio della trasmissione e con una lunghezza di 400 o 800 ns) tra una comunicazione e l'altra. All'interno dell'intervallo, si inserisce il *Cyclic prefix*, che consiste nella ripetizione dell'ultima parte della comunicazione avvenuta precedentemente. Questa ripetizione è necessaria per ottimizzare l'utilizzo della trasformata di Fourier (*FFT - Fast Fourier transform*) nelle fasi di modulazione e demodulazione. Infatti, il segnale codificato utilizzando l'OFDM per ciascun sotto-canale è descritto dal trasmettitore nel dominio delle frequenze; per essete trasmesso, viene quindi convertito nella corrispondente forma d'onda applicando l'*IFFT (Inverse FFT)*, mentre per essere riconvertito in segnali OFDM al ricevitore, verrà applicata la FFT che estrarrà l'ampiezza di ciascun sotto-canale.

3.2.1 Il livello fisico OFDM

Come descritto nel paragrafo relativo al livello fisico (PHY) nella sezione 2.3.1, anche la modulazione OFDM include la propria implementazione del PLCP, il cui frame (pacchetto di dati da trasportare) è mostrato in figura 3.5. Nella figura sono presenti tre varianti diverse (a,b,c) dello stesso frame corrispondenti alle tre diverse

implementazioni proposte negli standard 802.11a/g, 802.11n e 802.11ac. In ogni caso, per mantenere una retro-compatibilità, sia il frame descritto nell'802.11n che quello di nostro interesse descritto nell'802.11ac iniziano con gli stessi campi previsti dalla prima variante proposta.

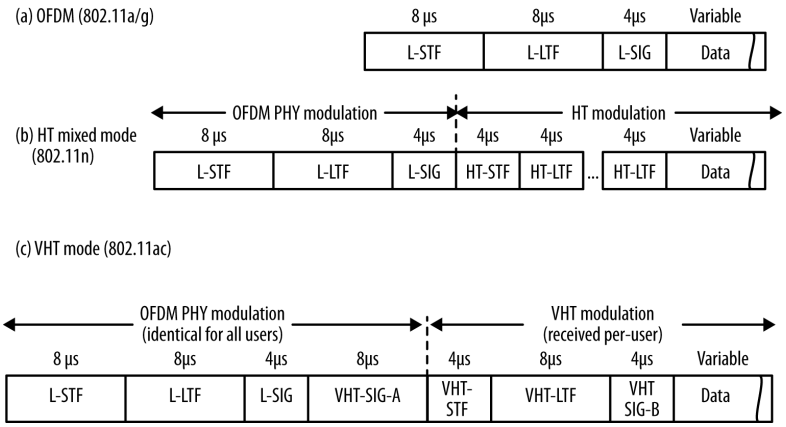

Figura 3.5: Formato del frame OFDM al livello fisico

I campi nel frame VHT (*very high throughput*: il nome assegnato ai frame di tipo 802.11ac) sono i seguenti:

1. *L-STF e L-LTF (short Training Field e Long Training Field)*: contengono rispettivamente una sequenza simboli OFDM e due simboli lunghi, che vengono utilizzati per assistere il ricevitore nell'identificazione di un frame OFDM, nella scelta dell'antenna e nella sincronizzazione.

2. *L-SIG (Signal Field)*: Usato per descrivere la lunghezza del frame in byte e la velocità di trasmissione, per permettere al ricevitore di calcolare il tempo necessario per ricevere tutto il frame.

3. *VHT-SIG-A e -B*: Sono l'equivalente del L-SIG ma sono comprensibili esclusivamente a dispositivi 802.11ac. Contengono informazioni relative all'ampiezza del canale, alla modulazione e alla codifica. Inoltre presentano variazioni nel caso in cui il frame sia destinato ad un solo utente o a più utenti contemporaneamente (grazie al MU-MIMO).

4. *VHT-STF*: Equivalente al L-STF, ma contiene informazioni esclusive per la versione VHT.

5. *VHT-LTF*: Equivalente al L-LTF, ma contiene informazioni esclusive per la versione VHT. Dipende dal numero di stream trasmessi.

6. *Data*: Contiene, tra le altre cose, il PSDU con i pacchetti creati ai livelli superiori.

Modulazione e Codifica

La scelta della velocità del collegamento, che dipende dal numero di stream impiegati e dalle interferenze presenti sul canale, è determinata dal *MCS (Modulation and Coding Set)*. Questo valore, che è in formato numerico e permette la scelta di 9 configurazioni diverse, mostrate nella tabella 3.1, determina sia la Modulazione utilizzata che il Code-rate.

MCS	Modulazione	Code-rate (R)
0	BPSK	1/2
1	QPSK	1/2
2	QPSK	3/4
3	16-QAM	1/2
4	16-QAM	3/4
5	64-QAM	2/3
6	64-QAM	3/4
7	64-QAM	5/6
8	256-QAM	3/4
9	256-QAM	5/6

Tabella 3.1: Valori MCS per 802.11ac

Modulazione In generale, per ottimizzare la trasmissione, non si usa codificare ciascun bit singolarmente, trasmettendo quindi un segnale con sole due variazioni (in ampiezza, in frequenza o in fase) per indicare il valore 0 o il valore 1, ma il dato atomico che viene trasferito prende il nome di *simbolo*, il quale al variare della complessità sarà traducibile in un certo numero di bit. Il quanto di tempo utilizzato per trasmettere un determinato simbolo è uniformemente predeterminato dalla modulazione in uso. Il numero di bit trasmissibile per ogni quanto di tempo è invece generalmente pari a $log_2(N)$, dove N rappresenta il numero totale di simboli che sono trasmissibili con la modulazione considerata.

Diagramma della costellazione Per rappresentare la modulazione del segnale viene utilizzato il *Diagramma della costellazione*. Questo diagramma giace sul piano bidimensionale complesso, Dove è possibile localizzare la posizione di ciascun simbolo come se fosse un punto nel diagramma.
La distanza del punto dall'origine rappresenta l'ampiezza (la potenza) del segnale,

mentre l'angolo (misurato in senso antiorario a partire dall'asse orizzontale, considerando il punto come se fosse l'estremita del vettore che lo connette all'origine) rappresenta la variazione in fase rispetto a un valore di riferimento.
A seconda del tipo di modulazione adottato si ottiene una costellazione differente, in figura 3.6 è mostrato a titolo d'esempio il diagramma in cui sono evidenziati i quattro punti corrispondenti ai quattro simboli trasmissibili con QPSK. La rap-

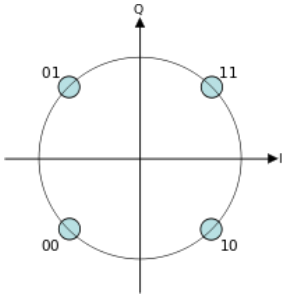

Figura 3.6: Diagramma della Costellazione per la modulazione QPSK

presentazione di un simbolo tramite un numero complesso si ottiene grazie ad una proprietà della sinusoide, la quale può essere a sua volta scomposta in due sinusoidi dove la prima prende il nome di *componente in-fase I* e la seconda, con una fase spostata di 90° (cioè un coseno), prende il nome di *componente di quadratura Q*. Considerando l'asse orizzontale del piano complesso come la componente I, mentre l'asse orizzontale come la componente Q e stampandovi dei numeri complessi così formati, si ottiene proprio il diagramma della costellazione.
Analizzando la comunicazione attraverso il diagramma della costellazione, nonostante il trasmettitore invii dei punti corrispondenti a simboli precisi, per via del rumore nel canale di comunicazione il ricevitore, interpretando il segnale sinusoidale tramite le relative componenti I e Q acquisisce dei punti simili a come mostrato nell'esempio in figura 3.7. Per ciascun punto acquisito, un demodulatore si occupa di effettuare una classificazione abbinandolo al relativo simbolo, scegliendo come criterio il simbolo della costellazione più vicino (*maximum likelihood*). Se il rumore e la quantità di interferenze presenti nel canale di comunicazione sono troppo elevati, il demodulatore classificherà erroneamente alcuni simboli, traducendo quindi un messaggio diverso da quello codificato dal trasmettitore. In presenza di modulazioni più aggressive che prevedono la trasmissione di più bit per ogni simbolo, è necessario che il rumore sia minimo per poter ottenere una classificazione corretta.

Di seguito sono descritte le tre tipologie di modulazione previste nello standard 802.11ac.

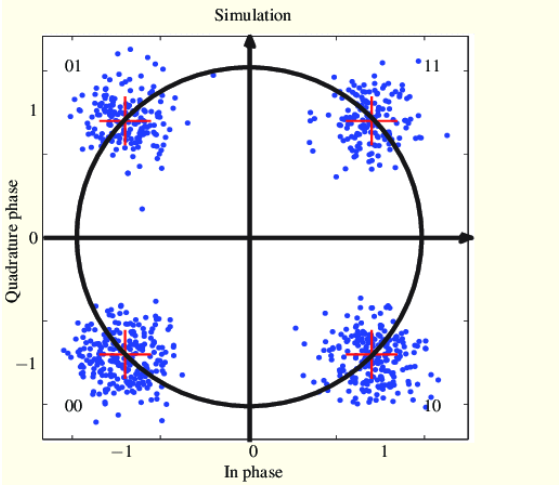

Figura 3.7: Valori ottenuti nel diagramma della costellazione durante un trasferimento di dati.

- *BPSK (Binary phase-shift keying)*: Il tipo di modulazione PSK consiste nel trasmettere le informazioni cambiando la fase di un segnale avente frequenza costante. La sua versione più semplificata, chiamata BPSK (o anche 2PSK) utilizza solo due fasi diverse, separate di 180° l'una dall'altra, per questo motivo BPSK trasmette esattamente un bit per ogni simbolo, dove una fase rappresenta il bit di valore zero e l'altra fase rappresenta l'uno.
  Nel diagramma della costellazione, le modulazioni PSK hanno tutti i simboli equidistanti dall'origine (dato che l'ampiezza non varia mai). Nello specifico, i due simboli usati da BPSK, essendo spaziati di 180° si trovano sull'asse orizzontale.

- *QPSK (Quadrature phase-shift keying)*: è anche chiamata 4PSK, in quanto utilizza quattro punti della costellazione, ciascuno con una variazione in fase di 90° (come mostrato nella figura 3.6). In questo caso, per ogni simbolo sono trasmessi due bit, e i quattro simboli servono per codificare le coppie di bit {00, 01, 10, 11}. In figura 3.8 si può vedere come varia la fase del segnale sinusoidale trasmesso al variare del simbolo corrispondente.

- *QAM (Quadrature Amplitude Modulation)*: Questo tipo di modulazione può essere visto come l'unione di una modulazione in fase (come nel caso di PSK) e una modulazione in ampiezza. In questo caso, non viene aprioristicamente definito il numero di simboli diversi che è possibile trasmettere, ma tipicamente, si tratta di una potenza del due (2, 4, 6, ..) dove l'esponente identifica a sua volta quanti siano i bit trasmessi da ciascun simbolo. Una conseguenza pratica di questo comportamento è che tipicamente i punti nella costellazione

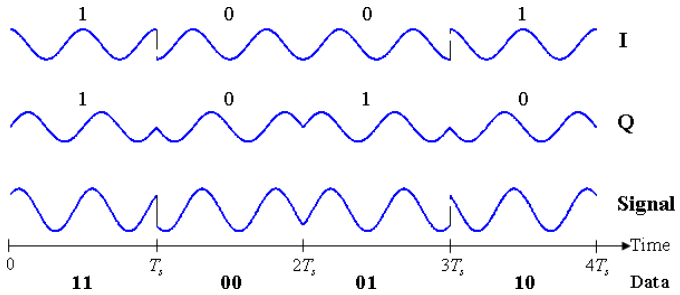

Figura 3.8: Segnale nel tempo modulato con QPSK al variare del simbolo (data) trasmesso

formano una griglia quadrata come mostrato in figura 3.9.

Per poter identificare specificatamente quale tipologia di modulazione è in

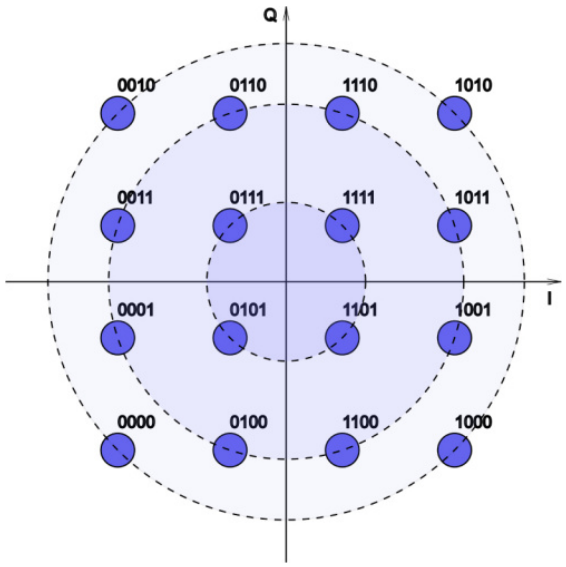

Figura 3.9: Diagramma della Costellazione per la modulazione 16-QAM

uso, si antepone al termine QAM il numero di simboli trasmissibili. Per esempio, una modulazione 16-QAM implica che si possano inviare sedici simboli diversi combinando quattro possibili configurazioni alternative di ampiezza con quattro possibili configurazioni di fase, generando quindi un quadrato 4x4 dove ogni simbolo corrisponde a una sequenza di 4 bit.

La codifica 256-QAM, inserita per la prima volta nello standard 802.11ac, consente di utilizzare 256 simboli diversi variando su sedici livelli di ampiezza e sedici di fase. Ciascun simbolo corrisponde a un byte (8 bit). Sulla falsa riga di quanto avviene con le modulazioni PSK, anche in questo caso aumen-

tare il numero di bit trasmessi per ogni simbolo aumenta sensibilmente la velocità di trasmissione ma richiede una notevole precisione in fase di demodulazione, imponendo che il numero e l'estensione degli errori sia minima.
Per concludere, nell'esempio in figura 3.10, sono mostrate le variazioni sia in fase che in ampiezza del segnale modulato con 8-QAM al variare di quattro simboli diversi (0, 6, 1 e 7), dove ciascun simbolo equivale a un messaggio di 3 bit.

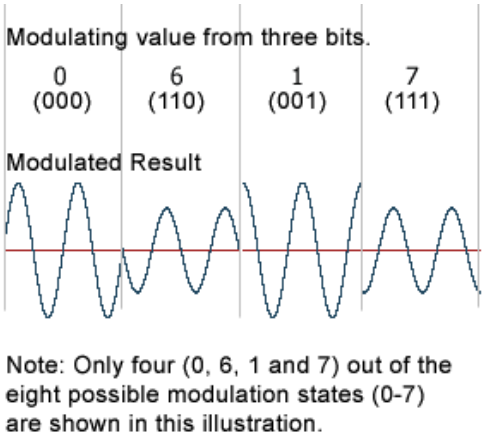

Figura 3.10: Segnale nel tempo modulato con 8-QAM al variare del simbolo (data) trasmesso. Sono trasmessi 4 simboli (0, 6, 1 e 7) corrispondenti ai bit (000, 110, 001, 111)

Code-rate Una parte dei bit trasmessi durante la comunicazione non viene utilizzato per trasmettere il messaggio ma per garantire ridondanza e correzione degli errori. La frazione di bit devoti a questa funzione prende il nome di code-rate. Utilizzare un code rate pari a $\frac{1}{2}$ significa che solamente metà dei bit inviati è effettivamente impiegata per trasmettere il dato vero e proprio, mentre l'altra metà è 'persa' per gestire la comunicazione.
Per ragioni di compatibilità con gli standard precedenti, e per garantire una inizializzazione corretta di ciascun pacchetto di dati, i primi campi del frame VHT in figura 3.5 (L-STF, L-LTF, L-SIG) sono tutti inviati con l'MCS più lento a disposizione: modulazione BPSK e $R = 1/2$, per una velocità pari a 6Mbps

3.2.2 Il Livello MAC

In questa sezione sarà principalmente descritta la composizione dei frame 802.11ac che incapsulano i pacchetti provenienti dal livello superiore, senza soffermarsi in

dettaglio su ciascun campo. Nella figura 3.11 è mostrato il formato generico del frame.

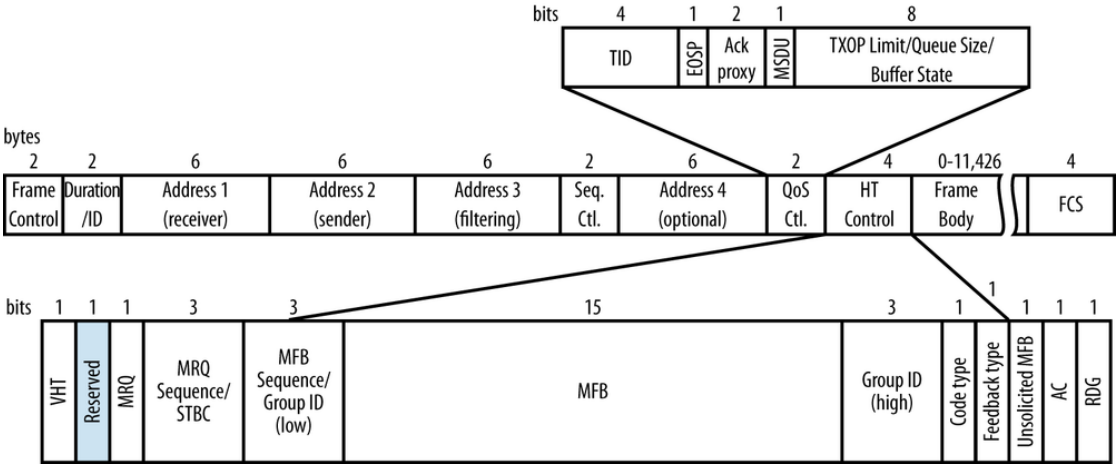

Figura 3.11: Il generico frame 802.11ac

Ciascun Frame è fondamentalmente composto da tre parti principali, identificate di seguito.

1. Il *MAC header*, che comprende la maggior parte dei campi visti nella figura 3.11: il Frame Control (figura 3.12), la durata, gli indirizzi e una serie di componenti opzionali.

2. Il *Frame body* di lunghezza variabile, che contiene informazioni specifiche al tipo di frame come la lunghezza massima dei campi MSDU, MDPU e la durata massima del PPDU.

3. L'*FCS (Frame check Sequence)* che contiene un CRC di 32-bit per identificare eventuali errori nel frame arrivato al destinatario, confrontando il valore presente nel campo con quello calcolato sui dati ricevuti.

Di seguito sono descritti alcuni campi presenti nell'header nel frame generico.

Frame Control field

È un campo di 16 bit che contiene una serie di proprietà:

1. *Protocol Version*: è fissato a zero per lo standard 802.11ac e tutti gli altri valori sono riservati. Nel caso in cui servisse introdurre una revisione incompatibile con quella attualmente esistente, sarebbe identificata da un protocol version diverso.

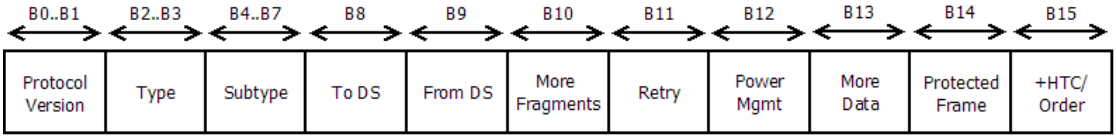

Figura 3.12: Contenuto del campo Frame Control

2. *Type e Subtype*: servono per identificare la funzionalità del frame. Esistono tre tipologie principali di frame: *Controllo*, *Data* e *Management*. Per ciascun tipo sono stati definiti una serie di sotto-tipi possibili.

    - La tipologia Data viene utilizzata per identificare i frame che trasmettono informazioni provenienti dai livelli superiori
    - La tipologia Management viene usata per la gestione della connessione, associazione, autenticazione e disconnessione dei dispositivi alla rete. Il sotto-tipo *Action*, inoltre, è usato per attivare una serie di ulteriori azioni e funzionalità di rete.
    - La tipologia di controllo viene usata per gestire l'accesso al mezzo di comunicazione e l'*acknowledgement* del frame, cioè l'invio della conferma da parte del destinatario della ricezione del messaggio.

3. *To DS e From DS*: hanno un significato diverso a seconda della tipologia del frame specificata. In generale sono utilizzati per identificare se tra il mittente o il destinatario della comunicazione vi è l'access point che gestisce la rete. Nei frame di Controllo non sono utilizzati.

4. *More Fragments*: Quando un pacchetto al livello MAC viene spezzettato in più frame al livello PHY, viene impostato a uno se il frame in questione è seguito da altri frame relativi allo stesso pacchetto MAC.

5. *Retry*: Impostato a uno se il frame è una ritrasmissione di un frame precedentemente inviato (Serve per permettere al ricevente di rimuovere eventuali duplicati).

6. *Power Management, More Data, Protected Frame, +HTC/Order*: Sono valori riservati o costanti durante tutta la trasmissione, Protected frame identifica frame il cui body è crittografato.

Duration/ID

Tipicamente utilizzato per indicare la durata nel tempo per la trasmissione del frame, in alcune tipologie particolari viene impostato con un valore fisso.

I campi Address (Indirizzi)

Ci sono quattro campi contenenti un indirizzo nel MAC frame, usati per indicare il *BSSID (Basic service set identifier)*, relativo all'infrastuttura di rete, l'indirizzo del mittente, del destinatario ed altri indirizzi opzionali in base al tipo di frame selezionato. Ciascun indirizzo è lungo 48 bit

Sequence Control

Non viene utilizzato nei frame di controllo. Presenta due sottocampi:

1. *Sequence Number*: 12 bit che servono ad identificare il numero sequenziale assegnato al relativo frame MAC.

2. *Fragment Number*: 4 bit che nel caso in cui il frame MAC sia stato spezzettato in più frame PHY servono per identificare l'ordine con cui ricomporre i frammenti. Nel caso in cui il frame non sia stato diviso, questo campo è impostato con il valore zero.

QoS Control

Sono informazioni relative al *Quality of Service*, per la gestione del traffico e la rimozione delle latenze

HT Control

Questo campo è stato inserito nello standard 802.11n e riutilizzato con l'802.11ac, anche se implementato con una variante diversa. Nella figura 3.11 viene mostrata la variante per l'802.11ac. Il primo bit *VHT* è impostato uguale ad uno se è in uso l'802.11ac, zero altrimenti. Nel resto dei campi presenti, si trovano informazioni relative all'mcs e l'ampiezza del canale consigliati.

3.3 MIMO: Multiple Input Multiple Output

Prima dell'introduzione dello standard 802.11n, sia il trasmettitore che il ricevitore hanno sempre utilizzato un'unica antenna durante la trasmissione[2], implementando così un sistema *SISO (Single-Input/Single-Output)*, traducibile in Singolo-ingresso/Singola-uscita. A partire dall'802.11n, invece, si è pensato di utilizzare il concetto dello *space diversity* (diversità spaziale), che consiste nell'uso di

[2]Anche nel caso in cui erano provvisti di più antenne, le quali venivano impiegate per la pratica dell'*Antenna Diversity*, che consiste nel scegliere per ciascuna comunicazione l'antenna migliore sulla base della potenza rilevata

più antenne sia al ricevitore che al trasmettitore, ciascuna localizzata in posizioni spaziali differenti. Così facendo, le onde elettromagnetiche trasmesse da ciascuna antenna del trasmettitore seguono un percorso differente - chiamato spatial stream (stream spaziale) - per raggiungere le antenne del ricevitore. Sistemi di questo tipo, che usano più antenne[3] contemporaneamente durante la comunicazione sfruttando lo space diversity, prendono il nome di sistemi *MIMO (Multiple-input/multiple-output)* - (Multiplo-ingresso/multipla-uscita). In figura 3.13 si possono vedere a titolo esemplificativo i diversi stream generati da una comunicazione SISO e da una comunicazione MIMO 2x2. Questa tecnologia non è esclusiva del Wi-Fi: viene infatti impiegata anche nelle reti cellulari LTE e in tanti altri sistemi di comunicazione senza fili.

I vantaggi ottenibili utilizzando MIMO sono:

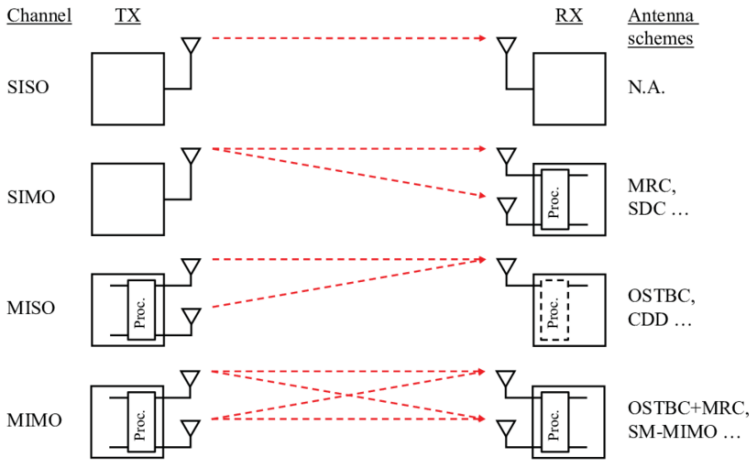

Figura 3.13: Trasmissione SISO, SIMO, MISO e MIMO

- L'aumento della velocità di comunicazione.
- Il miglioramento della stabilità nella comunicazione.
- Possibilità di eseguire il beamforming.

Le antenne usate da ciascun nodo sono tipicamente disposte parallelamente su di un asse ed equi-distanziate l'una dall'altra, formando un *array*. Il numero massi-

[3] In realtà, insieme all'antenna è necessario implementare anche tutto il resto dell'architettura e della componentistica necessarie al suo funzionamento in modo autonomo. L'insieme di questi dispositivi prende il nome di *radio chain*. Tra gli strumenti da inserire vi sono: amplificatori, convertitori analogico/digitali, mixers..

mo di antenne utilizzabili contemporaneamente in un array secondo lo standard 802.11ac è pari a 8.

La sintassi utilizzata per definire le capacità di un sistema MIMO è la seguente: $M \times N = Z$. Dove M identifica il numero di antenne usate dal trasmettitore durante la trasmissione, N il numero di antenne usate dal ricevitore e Z il numero di data stream effettivamente inviati dalle antenne. Per poter inviare x stream diversi, è necessario che M ed N siano maggiori o uguali di x, in quanto ogni data stream ha necessariamente bisogno di essere trasmesso e ricevuto da almeno un'antenna. La proprietà sfruttata dalla tecnologia MIMO è denominata *Multipath propagation*, e consiste nel fatto che lo stream trasmesso da una singola antenna omnidirezionale, può seguire diversi percorsi indipendenti (in base alla configurazione geografica) per raggiungere il ricevitore (figura 3.14). Tipicamente, uno di questi stream (quello più diretto) è in *line-of-sight*, cioè non incontra alcun ostacolo nel percorso dal trasmettitore al ricevitore, mentre gli altri tracciati raggiungono il ricevitore in un secondo momento, dopo una serie di rimbalzi. Questo comportamento, ha rappresentato un problema fino allo standard 802.11g: infatti, al ricevitore, l'unico segnale dominante supportato (tipicamente il line-of-sight) subiva un'interferenza distruttiva con l'arrivo degli altri segnali che aumentavano il rumore della comunicazione. Implementando il MIMO, invece, la multipath propagation viene sfruttata per trasmettere segnali diversi e non correlati l'uno con l'altro, di modo che il ricevitore possa facilmente distinguerli su ciascuna antenna e ricostruire il messaggio senza subire interferenza.

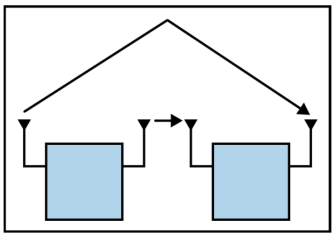

Figura 3.14: Esempio di una comunicazione multipath

STBC - Space-time block coding Se il motivo principale per cui è stato implementato il Mimo è avere un aumento nelle prestazioni di comunicazione, utilizzando lo STBC, invece, queste si mantengono invariate, ma si migliora la qualità e la portata della comunicazione. La tecnologia usata alla base è sempre la medesima, con la differenza che sui vari stream indipendenti vengono inviate copie dello stesso messaggio. Implementando questo formato di *diversity coding*,

al ricevitore è possibile combinare le informazioni ricevute per ottenere un segnale più chiaro e selezionare tra ciascuno stream quello più potente.

Le velocità di comunicazione teoricamente raggiungibili dallo standard 802.11ac dipendono da tanti dei numerosi fattori che abbiamo analizzato in questo capitolo: l'mcs selezionato, il numero di stream, il quanto di tempo impiegato come guardia tra una comunicazione e l'altra e l'ampiezza del canale. A titolo esemplificativo, la velocità minima disponibile è pari a 6.5Mbps, combinando un mcs pari a 0 (BPSK, R=1/2), un intervallo di guardia pari a 800ns, un solo stream spaziale e un canale ampio 20Mhz. La velocità massima invece è quasi 7Gbps, usando mcs uguale a 9 (256-QAM, R=5/6), intervallo di 400ns, 8 stream spaziali e canale ampio 160mhz.

MU-MIMO Un'aggiunta portata dallo standard 802.11ac al MIMO, è il Multi User MIMO (MIMO multi-utente). In seguito a questa introduzione, il MIMO tradizionale è stato chiamato anche SU-MIMO (single user, singolo utente). Il concetto utilizzato non è diverso da quanto avviene nella versione singola, con la differenza che i vari stream spaziali non sono tutti diretti allo stesso array di antenne ma sono diretti a dispositivi diversi, permettendo al trasmettitore di comunicare con più utenti nello stesso istante temporale.

Visto il notevole incremento tecnologico dovuto all'implementazione di tutti i nuovi requisiti richiesti dallo standard, si è ritenuto opportuno suddividere il rilascio dei dispositivi compatibili con l'802.11ac in due fasi distinte.
La prima fase, subito disponibile durante il lancio dello standard 802.11ac nel 2013 prevedeva i seguenti limiti allo standard:

- Canali di ampiezza massima pari a 80Mhz.
- Supporto massimo MIMO $3 \times 3 : 3$.
- Nessun supporto al MU-MIMO.
- Nessun supporto al Beamforming esplicito

La seconda fase, introdotta a partire dal 2016, sblocca tutte le potenzialità dello standard, anche se numerose funzionalità (come il supporto al beamforming, ai canali da 160Mhz, alla modulazione 256-QAM e a più di due stream), rimangono opzionali e la loro implementazione non è considerata obbligatoria per potervi aderire.

3.4 Il Processo di trasmissione e ricezione

In questa sezione, verrà descritto ad alto livello il processo di trasmissione di un pacchetto in arrivo dal livello MAC al livello PHY, alla luce delle informazioni acquisite fin'ora.

1. *PHY padding*: Vengono eventualmente aggiunti una serie di bit al termine del pacchetto in modo tale da poterlo suddividere in un numero intero di simboli, senza che l'ultimo di questi contenga meno bit di quanto previsto.

2. *FEC - Forward Error Correction*: Si applicano delle tecniche di riduzione degli errori manipolando e rimescolando i bit in ingresso secondo dei criteri opportuni.

3. *Divisione in stream* Nel caso in cui si utilizzi più di uno stream spaziale, i bit vengono divisi a seconda del corrispettivo stream

4. *Constellation mapping* I bit sono mappati nei corrispettivi simboli della costellazione (tipicamente secondo la modulazione QAM).

5. *STBC Opzionale.* In caso sia in uso, i simboli mappati in una costellazione sono copiati su più radio chains.

6. *Inserimento dei sotto-canali pilota e Cyclic shift diversity*: I simboli della costellazione sono combinati con le informazioni da inserire nei canali pilota. Nel caso ci siano più stream di dati, a ognuno di essi viene applicata una variazione ciclica di fase (CSD). Questa variazione serve a minimizzare la correlazione tra i diversi segnali inviati contemporaneamente.

7. Ciascun stream spaziale viene assegnato al relativo radio chain che si occuperà della trasmissione.

8. *IFFT*: I dati nel dominio delle frequenze (per via della modulazione OFDM) sono convertiti nel dominio del tempo per poter essere trasmessi.

9. *Intervallo di guardia*: All'inizio di ciascun simbolo viene inserito l'intervallo di guardia

10. Vengono costruiti i campi a preambolo del frame VHT (figura 3.5)

11. *Trasmissione*: Il dato da trasmettere è convertito in un segnale da piazzare al centro del canale assegnato. Si fa uso di amplificatori di potenza per migliorare il range del segnale, nei limiti imposti dal regolatore.

Il processo di ricezione è esattamente l'inverso di quanto appena descritto. Il segnale in arrivo viene processato da degli amplificatori a basso rumore, viene convertito al dominio delle frequenze diventando una serie di simboli della costellazione, che sono poi convertiti in bit e riprocessati dal FEC per correggere eventuali errori. Infine, sono passati al livello superiore (MAC) per la parte restante della catena di processamento e la decodifica del messaggio.

Capitolo 4

Il beamforming

Una caratteristica propria delle cosiddette antenne *direzionali* è quella di focalizzare la trasmissione in una zona specifica, determinata aprioristicamente durante la progettazione. L'uso di antenne direzionali viene spesso impiegato al fine di ottimizzare la potenza emessa durante la trasmissione, e permette al segnale di percorrere distanze più ampie prima di essere sopraffatto dal rumore. Ciononostante, in tutti i dispositivi Wi-Fi commerciali, considerando la relativa mancanza di stazionarietà e la necessità che funzionino nella maggior parte delle condizioni operative, si impiegano tipicamente delle antenne omnidirezionali, che emettono il segnale omogeneamente in tutto lo spazio che le circonda, formando una copertura a forma di cerchio. Una metafora che utilizza onde a frequenze diverse (luce visibile) per spiegare il funzionamento di queste due classi di antenne, cosi da poter risultare più famigliare, è mostrata in figura 4.1. La lampadina, che nell'esempio in questione assume il ruolo di sorgente omnidirezionale, è progettata per diffondere luminosità in tutta l'area circostante (una stanza). Una torcia, che invece prende il ruolo della sorgente direzionale, ha un fascio di luce più ristretto e concentrato nella direzione verso la quale viene puntata. Utilizzando una sorgente avente la stessa potenza luminosa per entrambe, la distanza entro cui l'ambiente circostante verrà illuminato dal fascio generato dalla torcia risulterà essere decisamente superiore rispetto a quanto ottenuto con la lampadina, al costo di lasciare il resto dell'ambiente circostante non illuminato.

Grazie all'introduzione del MIMO e l'uso di array di antenne per la comunicazione, tuttavia, è possibile ottenere un comportamento simile ad una antenna direzionale utilizzando la tecnica del *beamforming*, che è stata inserita negli standard 802.11 a partire dalla versione 802.11n. Usando il beamforming, quindi, si può focalizzare la stessa potenza che nel caso omnidirezionale verrebbe "sprecata" direttamente verso il ricevitore, consentendo così di poter utilizzare una modulazione più aggressiva, e di conseguenza ottenere velocità di comunicazione maggiori,

Figura 4.1: Diffusione Omnidirezionale e direzionale della luce

a parità di distanza dal trasmettitore. Inoltre, a differenza di un'antenna direzionale statica, utilizzare il beamforming consente di poter decidere attivamente come *sterzare* la comunicazione, focalizzando la trasmissione ora verso una direzione ora verso l'altra, adattandosi meglio ai contesti di mobilità tipici di una connettività mobile senza fili.
Durante la comunicazione tra due dispositivi Wi-Fi, tipicamente un Access Point (AP) e un Client ad esso connesso, ci si troverà d'innanzi a un flusso di dati che si muove dall'AP al client e uno inverso dal client all'AP. Il beamforming può essere configurato indipendentemente su ciascuna di queste due trasmissioni: non vi è alcuna imposizione sul fatto che debba essere usato contemporaneamente per entrambi i versi. Nel caso fosse impiegato, il dispositivo che si occupa della trasmissione del segnale prende anche il nome di *Beamformer*, mentre il dispositivo che si occupa della ricezione prende il nome di *Beamformee*. A riprova della possibile asimmetria nell'implementazione del beamforming, alcuni dispositivi in commercio sono in grado di prendere solamente uno di questi due ruoli, in base all'uso più tipico per cui sono stati progettati.

Beamforming implicito ed esplicito Nel contesto dello standard Wi-Fi 802.11, esistono due macro categorie di beamforming, che sono state entrambe introdotte a partire dallo standard 802.11n: il beamforming esplicito ed il beamforming implicito. La versione più utilizzata nell'802.11n è quella implicita, dove, non c'è bisogno di alcun scambio di dati dedicati alla sua configurazione, in quanto il beamformer si occuperà autonomamente di stimare come sterzare la comunicazione sulla base delle risposte ricevute e facendo inferenza sui frame che sono stati persi precedentemente. La totale mancanza di consapevolezza richiesta al beamformee per poter inizializzare ed esplicare questo tipo di ottimizzazione spiega il suo grande successo: è sufficiente che il beamforming sia supportato dal solo trasmettitore per essere utilizzabile con successo, non solo con dispositivi afferenti al medesimo standard, ma anche con nodi implementati secondo standard precedenti.
Il Beamforming esplicito, invece, prevede che ci sia una comunicazione attiva tra i due nodi al fine di determinare le caratteristiche del canale. Più nello specifico,

il beamformer si occupa di inviare un frame chiamato *sounding frame* al beamformee, il quale deve essere in grado di usare il frame ricevuto per misurare il canale e successivamente inviare il risultato al beamformer. Questa implementazione ha avuto poco successo nello standard 802.11n perché pochi dispositivi erano in grado di supportarla e lo standard non imponeva una metodologia univocamente condivisa, lasciando a ciascun produttore l'onere di progettare la propria versione, che spesso risultava essere incompatibile con ciò che era offerto dalla concorrenza.
Con l'avvento dello standard 802.11ac, al fine di superare questa criticità è stato chiaramente definito quali fossero le caratteristiche ed il comportamento previsto per ciascun nodo in grado di utilizzare il beamforming esplicito, dando così commercialmente vita anche a questo metodo.
Con l'introduzione del MU-MIMO, il beamforming viene anche utilizzato per poter focalizzare i differenti stream di dati verso ciascun dispositivo, facendo un uso ottimizzato della banda ed evitando mutue interferenze.

Il processo del beamforming può essere schematizzato nei seguenti questi passi:

1. Il beamformer trasmette un *Null Data Packet (NDP) Announcement frame.* La sua funzionalità è quella di prendere il controllo del canale di comunicazione. Infatti, le stazioni che ricevono questo frame smetteranno temporaneamente di occupare il canale per tutto il periodo in cui la procedura di sounding è in corso.

2. I beamformee che ricevono un NDP announcement frame rispondono al trasmettitore, in modo tale da permettergli di identificare i dispositivi abilitati al beamforming.

3. Il beamformer invia un NDP (o più di uno nel caso di MU-MIMO). Il Null data Packet (pacchetto con data nullo) è un pacchetto il cui body di livello 2 è privo di informazioni (figura 3.5c), mentre i campi dell'header sono impostati con dei valori predefiniti e conosciuti anche al beamformee.

4. I beamformee analizzano l'NDP effettivamente ricevuto, e confrontandolo con la versione originariamente trasmessa dal beamformer calcolano la risposta del canale $H_{eff,k}$, e di conseguenza la *feedback matrix* V_k, che viene inviata al trasmettitore. La risposta del canale è anche chiamata *CSI (Channel State Information)*, e fornisce informazioni relative a come l'onda elettromagnetica trasmessa dall'antenna Wi-Fi si propaga attraverso la superficie circostante, catturandone le attenuazioni in ampiezza e gli shift di fase.

5. Il beamformer utilizza la feedback matrix ricevuta per calcolare una steering matrix ($Q_{steer,k} = Q_k V_k$) dove Q_k è la matrice spaziale usata per configu-

rare l'NDP, che servirà a ridirigere la trasmissione verso la posizione del beamformee.

6. La procedura di sounding è conclusa, adesso il beamformer può applicare la steering matrix Q_{steer} durante le successive comunicazioni verso il beamformee.

Un esempio intuitivo di come applicando una steering matrix si possa modificare la comunicazione è presentato in figura 4.2. In questo caso, vedendo la figura 4.2(a), le tre antenne omnidirezionali trasmettono il segnale nello stesso istante e la trasmissione si irradia uniformemente nell'ambiente percorrendo la stessa distanza. Alternativamente, nella figura 4.2(b) è stato applicato uno shift di fase che ha portato ciascuna antenna a destra a trasmettere prima dell'antenna alla propria sinistra, con il risultato che ciascuna trasmissione sta adesso convergendo verso una specifica direzione. La steering matrix utilizzata nel beamforming, che rappresenta la descrizione matematica di come l'array del trasmettitore debba utilizzare ciascuna antenna per deviare la comunicazione verso un determinato percorso, segue lo stesso principio appena esemplificato, seppur introducendo una maggiore complessità.

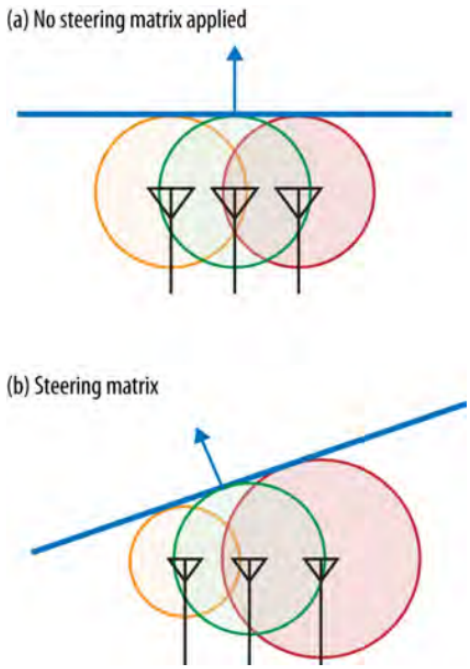

Figura 4.2: Esempio dell'utilizzo di più antenne per curvare la trasmissione.

Sebbene la scelta di utilizzare il beamforming esplicito possa sembrare banale, vista la sua abilità di migliorare la velocità di comunicazione, bisogna tenere in considerazione altri due fattori che combinati potrebbero inficiare i vantaggi derivati dall'utilizzo di questa tecnica:

- *Mobilità delle stazioni*: la connettività Wi-Fi è molto popolare su dispositivi portabili, come smartphone e portatili. In un ambiente in cui i beamformee non rimangono statici durante la trasmissione di informazioni è importante che il beamforming rimanga costantemente aggiornato, in quanto una steering matrix applicata parecchi istanti di tempo prima rispetto alla situazione attuale potrebbe amplificare la comunicazione lungo un percorso che non è più quello ottimale, che si è riconfigurato sulla base della nuova disposizione spaziale del ricevitore rispetto al trasmettitore.

- *Tempo impiegato durante la procedura del sounding*: Il sounding del canale per applicare il beamforming non è ottenuto "gratuitamente", ma richiede un lasso di tempo che viene sottratto alla comunicazione di dati.

È importante riuscire a bilanciare i due aspetti appena presentati: Aspettare troppo tempo tra un sounding e l'altro potrebbe mantenere in uso delle steering matrix obsolete per troppo tempo, che rallenterebbero la comunicazione. Al contrario, eseguire molti sounding potrebbe consumare troppa banda in relazione a quanto impiegato per eseguire la comunicazione.
Un decimo di secondo tra un sounding packet ed il successivo si è misurato essere un buon compromesso, considerando che a passo d'uomo si percorrono circa 17cm in quel lasso di tempo, e la steering matrix precedentemente calcolata è ancora utilizzabile. La procedura di sounding richiede circa 500 microsecondi ($500 * 10^{-6}$ secondi), cioè, in questo caso, consuma circa lo 0.5% del tempo dedicato alla comunicazione.

4.1 I frame utilizzati per il Beamforming Esplicito

In questa sezione verranno analizzati i principali frame utilizzati durante la comunicazione (e mostrati in figura 4.3) per configurare il beamforming per un singolo utente. Essendo il beamforming gestito interamente all'interno dello standard 802.11ac, i frame in questione non avranno alcun elemento proveniente dal livello 3 (o superiori) dello standard OSI.

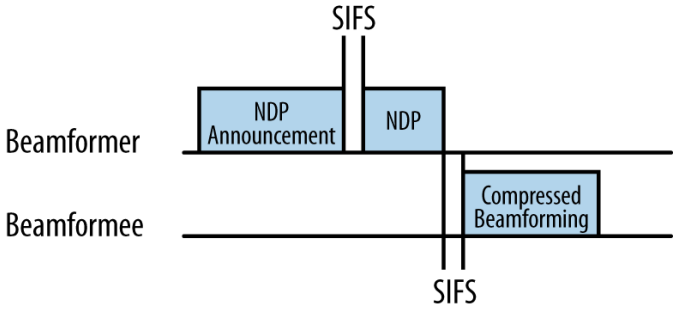

Figura 4.3: Frame scambiati durante la procedura di sounding

4.1.1 NDP Announcement Frame

Il Null Data Packet Announcement Frame è un frame di tipo controllo, in quanto la sua funzionalità è quella di bloccare temporaneamente l'accesso al mezzo di comunicazione agli altri dispositivi connessi. È mostrato in figura 4.4.

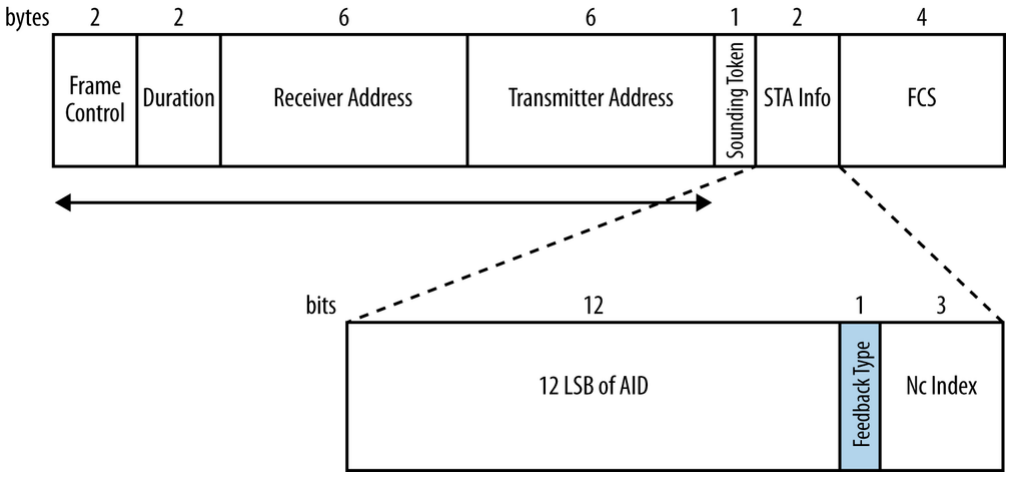

Figura 4.4: NDP Announcement Frame

- I primi campi previsti: Frame Control, Duration e gli Address, sono già stati descritti nella sezione 3.2.2, in quanto parte integrante del generico frame al livello MAC.
- Il *Sounding dialog Token Number* contiene un valore selezionato dal beamformer che serve ad identificare l'NDP Announcement frame.

- Il primo campo dello *STA Info*, contiene gli ultimi dodici bit (Least significative bits) dell'*AID (Association ID)* - ID di associazione, che viene assegnato a ciascun client nel momento della connessione con un Access Point (il quale ha un AID pari a zero).

- il bit di feedback type è uguale a zero se si sta impostando il beamforming nel caso SU (singolo utente), uno per il multi utente

- *Nc index*: Non viene utilizzato nel caso in cui il feedback type sia uguale a zero.

4.1.2 Null Data Packet Frame

Il Null Data Packet frame (figura 4.5) è un frame di tipo Data e sottotipo null, in quanto è equivalente al frame VHT OFDM presentato in figura 4.5 con data uguale a zero

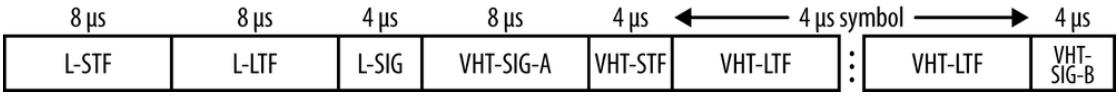

Figura 4.5: Null Data Packet

4.1.3 Compressed Beamforming Frame Action field

Il Compressed Beamforming Frame Action field (figura 4.6) è un frame ti tipo Management e sotto tipo Action no ACK (identificato col numero 14) che contiene la feedback matrix che il beamformee invia al beamformer.

Nella prima implementazione del beamforming con lo standard 802.11n erano previsti tre metodi diversi per inviare la feedback matrix:

- *CSI Feedback*: Il beamformee misura la CSI H_{eff} per ogni sotto-canale, rimuove i CSD (variazione ciclica di fase) applicati durante la trasmissione ed invia il risultato al beamformer senza fare altre elaborazioni. In questo caso spetterà quindi al beamformer l'onere di calcolare la feedback matrix.

- *Noncompressed beamforming feedback matrix*: Il beamformee, dopo aver rimosso i CSD applicati durante la trasmissione, calcola ed invia al beamformer le feedback matrix V_k, una per ogni sotto-canale.

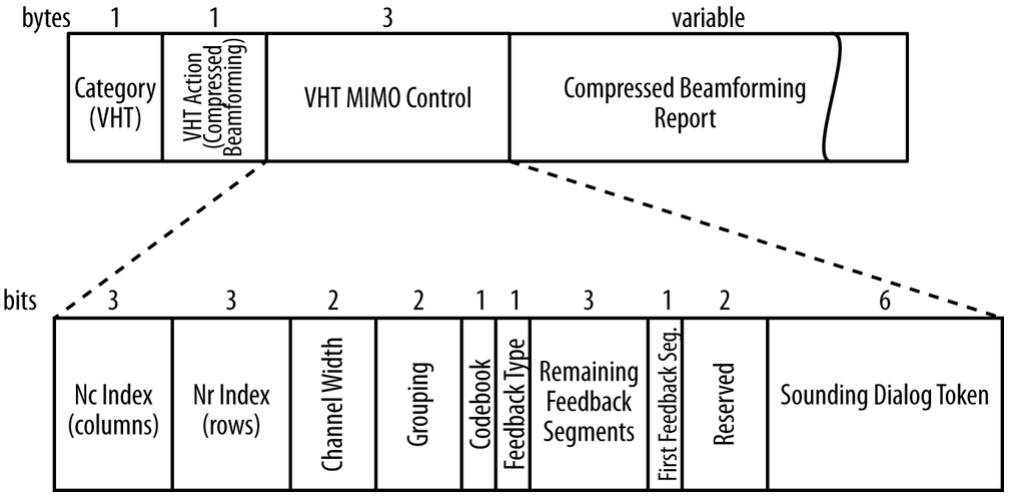

Figura 4.6: Compressed Beamforming Frame Action field con zoom su VHT MIMO Control

- *Compressed beamforming feedback matrix*: il beamformee, dopo aver rimosso i CSD applicati durante la trasmissione, calcola le feedback matrix V_k, una per ogni sotto-canale k. Successivamente, comprime ciascuna matrice in una serie di angoli, che saranno poi inviati al beamformer. Il beamformer, dopo aver effettuato la decompressione degli angoli e aver ricostruito le matrice V_k, calcola le relative steering matrix Q_k.

Nel processo di semplificazione del beamforming per lo standard 802.11ac, è stato mantenuto solamente l'ultimo metodo, quindi ogni report inviato contiene una compressed beamforming feedback matrix.

I Componenti del Compressed Beamforming Frame Action field sono:

- *Category*: La presenza di questo campo è prevista per tutti i frame Action No Ack e identifica la categoria specifica del frame in trasmissione, che nel caso del beamforming corrisponde al codice 21, dedicato a tutti i frame VHT.

- *VHT Action*: La presenza di questo campo è prevista per tutti i frame con Categoria VHT. L'action con il valore zero corrisponde al VHT Compressed Beamforming.

- *VHT MIMO Control*

- *Compressed Beamforming Report*

VHT MIMO Control

Questo campo viene utilizzato per definire le informazioni a contorno della feedback matrix che viene inviata. I campi di cui è composto sono mostrati nella figura 4.6 e descritti di seguito:

- *NC Index*: Indica il numero di colonne della compressed feedback matrix meno uno (Impostato a 0 se la matrice ha una colonna).
- *Nr Index*: Indica il numero di righe della compressed feedback matrix meno uno. (Impostato a 0 se la matrice ha una riga).
- *Channel Width* - Ampiezza del canale: Indica quanto è ampio il canale usato durante il sounding. è composto da 2 bit, si imposta uguale a 0 per un canale di 20Mhz, uguale a 1 per 40Mhz, 2 per 80Mhz e 3 per 160Mhz. Questa informazione è necessaria perché con un canale più ampio ci sono più sotto-canali, e quindi la feedback matrix sarà più grande.
- *Grouping*: É una tecnica per diminuire la dimensione del frame trasmesso quando la feedback matrix ha alcune porzioni che si ripetono in più punti diversi. Viene impostato a zero nel caso in cui non si utilizzi.
- *Codebook Information*: Definisce il numero di bit utilizzati per codificare ciascun angolo. La feedback matrix contiene due famiglie di angoli diversi: ψ e ϕ. Se è impostato a zero allora sono stati usati due bit per codificare ψ e 4 per ϕ, mentre se è impostato a uno sono stati usati quattro bit per ψ e sei per ϕ. Il numero di bit previsto cambia nel caso in cui il feedback type sia MU.
- *Feedback type*: impostato a zero se il report è SU, uno se è MU.
- *Remaining Feedback Segments*: Viene usato nel caso in cui la feedback matrix sia troppo larga per essere inviata con un singolo frame, per ordinare e gestire i vari frame in transito.
- *Sounding Dialog Token Number*: Ci si scrive lo stesso token ricevuto dal beamformer nel NDP Announcement Frame.

Compressed Beamforming Report field

Il Compressed Beamforming Report field contiene gli angoli veri e propri generati a partire dalla feedback matrix. La dimensione di questo campo dipende dai valori inseriti nel VHT MIMO Control. Insieme agli angoli vengono inseriti in testa al campo anche gli *SNR - Signal to Noise Ratio* ricevuti dal beamformee per ogni space-time stream. Per ciascun SNR vengono dedicati 8 bit.

4.2 Calcolo del Compressed report

4.2.1 Calcolo della feedback matrix V

La matrice H_{eff}, che rappresenta la CSI del sotto-canale, ha una dimensione pari a Nr (numero di antenne al ricevitore) × Nc (numero di antenne al trasmettitore) e contiene valori complessi.
Matematicamente, la si esprime nel seguente modo:

$$y = H_{eff}\ x + n \tag{4.1}$$

dove y è il segnale ricevuto (Nr), x il segnale trasmesso (Nc), n il rumore gaussiano. Per ottenere la feedback matrix V si calcola la fattorizzazione *SVD (Singular Value Decomposition)* - Decomposizione ai valori singolari - della matrice H_{eff}. L'output di questa fattorizzazione produce tre matrici U, S e V tali che

$$USV = H_{eff} \tag{4.2}$$

dove S è una matrice diagonale contenente i valori singolari di H_{eff} ordinati in senso decrescente, mentre U e V sono due matrici quadrate unitarie contenenti i vettori singolari ortogonali sinistro e destro. La dimensione di V è pari al numero di colonne di H_{eff} (Numero di antenne al trasmettitore). Per trasmettere n data stream spaziali, la scelta ottimale consiste nel trasmettere lungo i primi n vettori principali, perciò la feedback matrix verrà costruita prendendo le prime n colonne della matrice V[1]. Come specificato nello standard, il numero di stream deve essere necessariamente inferiore al numero di antenne impiegate nella trasmissione sia dal trasmettitore che dal ricevitore.
Una volta che il sounding è stato completato (e quindi il beamformer ha ottenuto V), il segnale da trasmettere viene calcolato secondo questa formula:

$$x = Vu \tag{4.3}$$

dove u è il segnale originale in assenza di beamforming.
Il ricevitore, che una volta effettuata la fattorizzazione mantiene in memoria la matrice U, ricostruisce il segnale originale con la formula:

$$u = Uy \tag{4.4}$$

[1]In definitiva, quindi, la matrice V ha un numero di righe pari al numero di antenne al trasmettitore e un numero di colonne pari al numero di stream spaziali.

4.2.2 Calcolo degli angoli relativi a ciascuna feedback matrix

Come anticipato, il beamformee non invia l'intera matrice V ma ne produce una versione compressa rappresentata da angoli. Prima di poter applicare la compressione sulla matrice V da inviare (che da ora in poi sarà chiamata $\tilde{V}$) è necessario applicare un ulteriore passaggio descritto dall'equazione $V = \tilde{V}\tilde{D}$, dove $\tilde{D}$ è una matrice diagonale del tipo $\tilde{D} = diag(e^{j\theta_1}, e^{j\theta_2}, e^{j\theta_{N_C}})$ che applica uno shift di fase. Gli angoli θ_i vanno scelti in modo tale che l'ultima riga di V sia non negativa e reale.
La compressione della V appena calcolata avviene grazie alla seguente proprietà. Una matrice unitaria $V \in \mathbb{C}^{Nr \times s}$, può essere rappresentata come:

$$V = \prod_{i=1}^{s} \left[D_i(1_{i-1} \quad e^{j\phi_{i,i}} \quad ... \quad e^{j\phi_{s-1,i}} \quad 1) \prod_{l=i+1}^{Nr} G_{li}^{T}(\psi_{li}) \right] \times I_{Nr \times s} \tag{4.5}$$

Dove $D_i(1_{i-1} \quad e^{j\phi_{i,i}} \quad ... \quad e^{j\phi_{s-1,i}} \quad 1)$ è una matrice quadrata $Nr \times Nr$ diagonale come mostrato nell'equazione 4.6, in cui 1_{i-1} rappresenta una sequenza di uni lunga i-1.

$$D_i(1_{i-1} \quad e^{j\phi_{i,i}} \quad ... \quad e^{j\phi_{s-1,i}} \quad 1) = \begin{bmatrix} 1_{i-1} & 0 & \dots & \dots & 0 \\ 0 & e^{j\phi_{i,i}} & 0 & \dots & 0 \\ \vdots & 0 & \ddots & 0 & 0 \\ \vdots & \vdots & 0 & e^{j\phi_{s-1,i}} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.6}$$

La matrice $G_{li}(\psi)$ è la matrice quadrata $Nr \times Nr$ utilizzata per effettuare la *rotazione di Givens*[2] come mostrato nell'equazione 4.7.

$$G_{li}(\psi) = \begin{bmatrix} I_{i-1} & 0 & 0 & 0 & 0 \\ 0 & \cos(\psi) & 0 & \sin(\psi) & 0 \\ 0 & 0 & I_{l-u-1} & 0 & 0 \\ 0 & -\sin(\psi) & 0 & \cos(\psi) & 0 \\ 0 & 0 & 0 & 0 & I_{N_r-1} \end{bmatrix} \tag{4.7}$$

I_m è una matrice identità m × m. $\cos(\psi)$ e $\sin(\psi)$ sono localizzati nella riga l e colonna i.

[2]Dal matematico *Wallace Givens* che l'ha introdotta per la prima volta nel 1950

Per esempio, la rappresentazione di una matrice V 4×2 è la seguente:

$$V = \begin{bmatrix} e^{j\phi_{11}} & 0 & 0 & 0 \\ 0 & e^{j\phi_{21}} & 0 & 0 \\ 0 & 0 & e^{j\phi_{31}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} \cos\psi_{21} & \sin\psi_{21} & 0 & 0 \\ -\sin\psi_{21} & \cos\psi_{21} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}^T \times \begin{bmatrix} \cos\psi_{31} & 0 & \sin\psi_{31} & 0 \\ 0 & 1 & 0 & 0 \\ -\sin\psi_{31} & 0 & \cos\psi_{31} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}^T \times \begin{bmatrix} \cos\psi_{41} & 0 & 0 & \sin\psi_{41} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -\sin\psi_{41} & 0 & 0 & \cos\psi_{41} \end{bmatrix}^T$$
$$\times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{j\phi_{22}} & 0 & 0 \\ 0 & 0 & e^{j\phi_{32}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\psi_{32} & \sin\psi_{32} & 0 \\ 0 & -\sin\psi_{32} & \cos\psi_{32} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}^T \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\psi_{42} & 0 & \sin\psi_{42} \\ 0 & 0 & 1 & 0 \\ 0 & -\sin\psi_{42} & 0 & \cos\psi_{42} \end{bmatrix}^T \times \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \tag{4.8}$$

O, utilizzando i nomi assegnati alle varie matrici:

$$V = D_1 G_{21}^T G_{31}^T G_{41}^T \times D_2 G_{32}^T G_{42}^T \times I_{42} \tag{4.9}$$

La procedura per scomporre la matrice V presenta delle similitudini con la fattorizzazione QR. Un'iterazione i (riga dell'equazione 4.8) viene eseguita nel seguente modo:
La presenza della matrice D nella moltiplicazione serve per estrarre le fasi della colonna i-sima, successivamente, utilizzando ogni matrice ortogonale della rotazione di Givens per rendere nullo un elemento al di fuori della diagonale, si annullano tutti gli elementi della colonna i-sima diversi dall'elemento principale, che assumerà il valore uno. Di conseguenza, considerando che le colonne di V sono tra di loro ortogonali, anche tutti gli altri elementi della riga i-sima assumeranno il valore nullo.
All'iterazione k, ciò che si ottiene moltiplicando V al risultato è una matrice le cui prime k righe e k colonne hanno tutti uni sulla diagonale principale e zeri altrove, mentre il resto della matrice è uguale alla sotto-matrice V_k a cui sono state rimosse le prime k righe e colonne. Dopo n iterazioni (nel caso di V 4x2, n = 2) l'algoritmo si può fermare in quanto per effetto della moltiplicazione finale per $I_{Nr\times s}$ si annulla tutta la sotto-matrice V_n rimanente. Nella seguente equazione, è mostrato a titolo esemplificativo il risultato della seconda iterazione per una matrice V di dimensioni generiche. Da notare come, essendo la seconda iterazione, siano state diagonalizzate solamente le prime due righe (colonne), e sia ancora presenta la sottomatrice V_3

$$(G_{N_r,2} \dots G_{32} D_2)(G_{n_r 1} \dots G_{31} G_{21} D_1) \times V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & & \\ 0 & 0 & & V_3 \end{bmatrix} \tag{4.10}$$

La matrice di feedback V può quindi essere completamente descritta dagli angoli appena determinati (Nell'esempio sono dieci: $\phi_{11}, \phi_{21}, \phi_{31}, \psi_{21}, \psi_{31}, \psi_{41}, \phi_{22}, \phi_{32}, \psi_{32}, \psi_{42}$), dove ϕ rappresenta le differenze relative di fase e ψ rappresenta le differenze relative di ampiezza.
Gli angoli ottenuti vanno poi quantizzati utilizzando le seguenti equazioni:

$$\psi = \frac{k\pi}{2^{b_\psi+1}} + \frac{\pi}{2^{b_\psi+2}} \tag{4.11}$$

$$\phi = \frac{k\pi}{2^{b_\phi-1}} + \frac{\pi}{2^{b_\phi}} \tag{4.12}$$

dove $k = 0, 1, \ldots, 2^{b_{\phi(\psi)}} - 1$ e b è il numero di bit usati per quantizzare l'angolo, determinato dal campo codebook del VHT MIMO Control.
Il motivo per cui le due famiglie di angoli utilizzano un numero di bit diverso per la quantizzazione è dovuto al fatto che ϕ varia da 0 a 2π mentre ψ da 0 a $\pi/2$: utilizzando quattro bit per ψ si hanno a disposizione 2^4 (16) valori diversi, mentre per ψ sono 2^6 (64), cioè esattamente il quadruplo. Considerando che anche 2π è esattamente il quadruplo di $\pi/2$, usando 2 bit in più per ψ si ottiene la stessa granularità durante la quantizzazione, cioè tra un valore rappresentabile e l'altro lo step per entrambi gli angoli è il medesimo.

4.2.3 Dimensioni totali del Compressed beamforming report

Come anticipato, per ogni space stream viene comunicato l'SNR con una dimensione di 8 bit.
Gli angoli, vengono trasmessi esattamente nell'ordine in cui vengono calcolati durante la procedura iterativa esemplificata nel capitolo precedente, e non vi è alcun padding o controllo che garantisca che la dimensione del report sia un multiplo esatto di un byte.
Ogni feedback matrix ha una dimensione pari a $N_a \times (b_\phi + b\psi)/2$, dove N_a è il numero di angoli usati, b_ϕ il numero di bit usati per quantizzare l'angolo ϕ e b_ψ il numero di bit usati per quantizzare l'angolo ψ
Si invia una feedback matrix per ogni sotto-canale presente, ad esclusione dei sotto-canali pilota e del canale centrale (0).
Considerando per esempio un canale di ampiezza pari a 20Mhz, codebook pari a uno, MIMO $4 \times 2 : 2$, la dimensione del report è:

$$8 * 2 + 52 * (10 * (6 + 4)/2) = 2616 \text{ bit} = 327 \text{ byte}$$

Dovuto dal fatto che ci sono due space stream, il numero di sotto-canali usati è 52, il numero di angoli per ogni feedback matrix è 10 e i bit usati per i due angoli sono sei e quattro.

Capitolo 5

Implementazione del Beamforming

La strategia più diretta per poter manipolare la radiazione emessa dal trasmettitore attraverso il beamforming sarebbe quella di operare esclusivamente su quest'ultimo, implementando all'interno dello stesso dispositivo un sistema in grado di costruire ed utilizzare una feedback matrix scelta dall'utente. Un approccio di questo tipo avrebbe però richiesto una profonda analisi e revisione del firmware usato dal trasmettitore, e probabilmente avrebbe comportato problemi di compatibilità tra diversi produttori o peggio tra ciascun modello diverso. La strada che è stata scelta in questa tesi, dunque, ripercorre tutta la procedura prevista dal beamforming e influenza la radiazione del trasmettitore indirettamente, utilizzando le informazioni opportunamente inserite nel Compressed report. In questo modo è possibile riconfigurare qualsiasi trasmettitore in grado di operare come Beamformer, mentre è necessario introdurre delle modifiche al firmware del dispositivo che prende il ruolo di Beamformee, al fine di trasmettere il report costruito dall'utente e non quello calcolato genuinamente dal dispositivo. Framework di questo tipo, che permettono l'iniezione di trame Wi-Fi inserite a partire dallo spazio utente su dispositivi commerciali, sono già conosciuti ed utilizzati nella letteratura specializzata e quindi si sono rivelati la via più conveniente da intraprendere. Nonostante la loro disponibilità, tuttavia, non sono mai stati utilizzati per l'iniezione di compressed report, in quanto l'operazione in questione richiede che il report sia inviato al beamformer in un istante di tempo molto preciso, dopo la ricezione del NDP. Questo aspetto, impone una profonda attività di reverse-engineering per poter intervenire nel firmware del chip radio proprio quando è in corso la fase di costruzione ed invio del report, ed è la ragione per la quale il sistema implementato nella tesi ci risulta essere il primo a percorrere questa strada.

5.1 Creazione del Compressed Beamforming report

Il primo requisito per poter configurare il beamforming tra due stazioni utilizzando degli angoli diversi da quanto misurato dalla procedura del sounding è quello di poter generare dei Compressed Beamforming report via software, che successivamente potranno essere utilizzati per influenzare a piacimento la generazione della steering matrix al beamformer.

Nella creazione del software, si suppone che le informazioni relative al tipo di canale in uso ed il file contenente tutti gli angoli da inviare siano dati in input.

Il linguaggio di programmazione utilizzato per costruire il report è *Matlab*, questa scelta è nata per via del fatto che MathWorks fornisce una serie di add-ons ufficiali utilizzabili per impostare e gestire le comunicazioni Wi-Fi con lo standard 802.11 (esempio: WLAN Toolbox). In ogni caso, per generare un compressed report è sufficiente produrre un file binario che rispetti la descrizione fornita dallo standard, quindi è possibile utilizzare un qualunque altro linguaggio di programmazione.
Nelle figure 5.1 e 5.2 sono mostrati rispettivamente i dettagli e il corrispondente codice esadecimale di un pacchetto generato dal software per la creazione del report e salvato in un file *PCAP (Packet Capture)* visualizzabile con il software *Wireshark*.
Come descritto nelle sezioni 3.2.2 e 4.1.3, i primi campi inseriti descrivono il tipo del

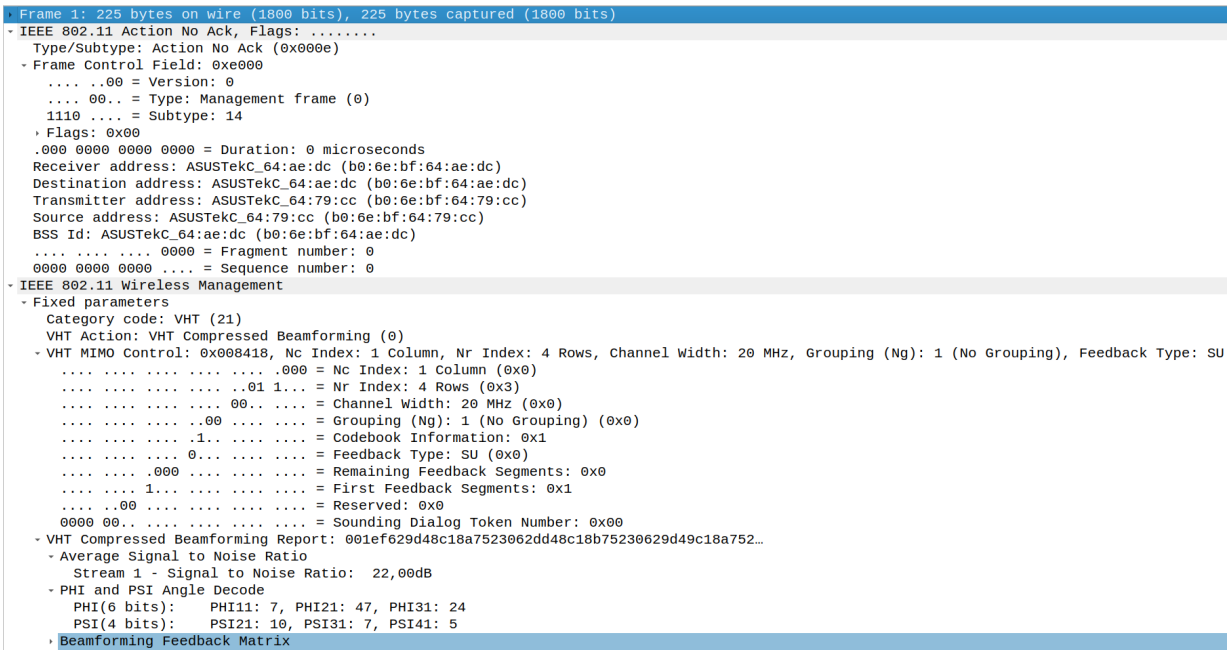

Figura 5.1: Esempio di un Compressed Beamforming Frame generato da Matlab e visualizzato su Wireshark

frame (Management) ed il sotto-tipo (Action No Ack), rappresentati dai primi due byte in codice esadecimale {`0xE0 00`}. Successivamente vi sono i campi degli indirizzi. Questa prima sezione corrisponde ai byte evidenziati in blu nella figura 5.2 e ha sempre una dimensione fissa, pari a 24 byte.
Nella sezione successiva, IEEE 802.11 Wireless Management, è contenuto il resto del pacchetto. In primis, è specificato il tipo (VHT - corrispondente al codice 21) ed il sotto tipo (Compressed report - 0) del Management Frame, identificati dall'esadecimale {`0x15 00`}. Successivamente sono presenti i sei bit del VHT MIMO Control. Nel caso analizzato in

```
0000  e0 00 00 00 b0 6e bf 64  ae dc b0 6e bf 64 79 cc
0010  b0 6e bf 64 ae dc 00 00  15 00 18 84 00 00 1e f6
0020  29 d4 8c 18 a7 52 30 62  dd 48 c1 8b 75 23 06 29
0030  d4 9c 18 a7 52 30 62 9d  49 c5 8a 75 27 16 29 d4
0040  9c 58 a7 52 71 62 9d 49  c5 8a 75 2b 16 29 d4 ac
0050  58 a7 52 b2 62 9d 4a c9  9a 75 2f 26 69 d4 ac 98
0060  a7 52 f2 66 9d 4a c9 9a  75 2f 26 65 d4 bc 99 97
0070  52 f2 66 5d 4a c9 99 75  2b 26 65 d4 ac 59 87 52
0080  f2 66 1d 4a c5 98 75 2b  16 61 d4 bc 59 87 52 f1
0090  66 19 0a c5 98 64 2b 16  5d 90 ac 19 76 42 b0 65
00a0  d9 0a c1 97 54 27 06 1d  50 9c 19 75 42 70 61 d5
00b0  09 c1 97 54 26 f6 5d 4c  9c 19 75 32 70 65 d4 c9
00c0  c1 97 53 26 f6 1d 4c 8b  d8 75 32 6f 66 14 c9 bd
00d0  88 53 27 06 21 4c 9c 19  85 32 2f 66 14 c8 bd 98
00e0  53
```

Figura 5.2: Esempio di un Compressed Beamforming Frame generato da Matlab e visualizzato su Wireshark in formato esadecimale

figura, il trasmettitore utilizza un array composto da quattro antenne e sta trasmettendo un solo space stream, l'ampiezza del canale è pari a 20Mhz ed il beamforming è singolo utente. L'ultima parte del pacchetto contiene il VHT Compressed Beamforming Report, di ampiezza variabile a seconda delle informazioni contenute nel VHT MIMO Control. Nel report vi è un solo SNR relativo all'unico Stream, seguito dalla lista di angoli ϕ e ψ. Per un sistema a 4 antenne ed uno stream sono previsti sei angoli per ogni feedback matrix. Al momento, nella versione utilizzata, Wireshark mostra in un formato decodificato unicamente gli angoli della prima matrice, utilizzando un ordine diverso da quanto previsto nello standard, inoltre, il metodo utilizzato per decodificarli in valori decimali, non rispecchia quanto ci si possa aspettare intuitivamente dalla misura di un angolo: in altre parole, $\phi_{11} = 7$ non significa che l'angolo ϕ_{11} è un angolo di sette gradi, ma significa che tra i 64 (2^6) valori possibili (tra 0 e 2π) dopo la quantizzazione lineare mostrata nell'equazione 4.12, ϕ_{11} è il settimo. Per questi due motivi, in generale, gli angoli qui esplicitati non sono da ritenersi attendibili rispetto a quando veramente codificato nel pacchetto.
La dimensione complessiva del frame è pari a 225 byte ($24+2+3+1+195$) scomponibile nel seguente modo:

1. I primi 24 byte di header per identificare il pacchetto
2. i due byte per la categoria del frame e i 3 byte per il VHT MIMO Control
3. La parte variabile: il byte per l'SNR dello stream e $52 * (6 * (6 + 4)/2) = 1560$ bit (195 byte) per il report.

Limitazioni e commenti sullo script per costruire il Beamforming report

- Può configurare beamforming report unicamente nel caso SU, e non in modalità multi utente.

- L'unico codebook accettato è quello uguale a 1, ossia la versione che prevede di quantizzare gli angoli con il maggior numero di bit.
- Accetta canali da soli 20Mhz.
- È in grado di gestire qualsiasi configurazione MIMO, fino alla $8 \times 8 : 8$.

Le estensioni che permettono di ampliare i canali accettati ad ogni ampiezza, e di utilizzare un codebook pari a zero sono facilmente implementabili, per quanto riguarda invece il MU beamforming, che consente al beamformer di trasmettere a più dispositivi in ricezione nello stesso istante di tempo, il formato di tutti i frame usati durante le fasi del sounding cambia, e anche nel caso del beamforming report è necessario aggiungere un campo in più rispetto a quanto esposto in questa tesi.

5.2 Generazione degli angoli per il Compressed Report

Una volta ottenuta la capacità di generare un compressed report, è necessario avere un metodo o una sorgente dalla quale estrarre tutti gli angoli che andranno a comporlo.
I modi con cui abbiamo ottenuto queste informazioni sono molteplici:

- Generazione degli angoli a partire dalla simulazione di una comunicazione Wi-Fi via software.
- Generazione degli angoli a partire da una CSI (misura del canale di comunicazione).
- Generazione degli angoli a partire dalla loro formulazione prevista dallo standard.

5.2.1 Generazione degli angoli a partire dalla simulazione di una comunicazione Wi-Fi via software

Anche in questo caso, per simulare il canale di comunicazione è stato utilizzato Matlab. Di seguito sono presentati i passi seguiti dallo script:

1. Generazione del NDP packet.
2. Simulazione del canale ed invio del NDP packet.
3. Generazione delle CSI al beamformee e compressione in angoli.

Generazione del NDP packet Per generare questo pacchetto, è stato utilizzato l'add-on di Matlab *WLAN Toolbox*, grazie al quale, tramite la classe `wlanVHTConfig` e la funzione `wlanWaveformGenerator`, è possibile generare un frame 802.11ac sulla base delle configurazioni date in ingresso (MCS, ampiezza del canale, numero di antenne al trasmettitore) e la relativa forma d'onda VHT. Come previsto dallo standard, per

misurare le CSI è necessario utilizzare un pacchetto specifico chiamato NDP. La classe `wlanVHTConfig` non dispone di un comando per poterlo generare automaticamente, ma è sufficiente creare un pacchetto qualsiasi su cui impostare un numero di space-time stream uguale al numero di antenne del trasmettitore, indipendentemente da quanti stream si intendono utilizzare effettivamente durante le comunicazioni successive, e il cui campo data sia assente (su matlab, impostandone la lunghezza uguale a zero).

Simulazione del canale ed invio del NDP packet Nel WLAN Toolbox sono a disposizione degli strumenti tramite i quali è possibile simulare realisticamente un canale di comunicazione aggiungendoci il relativo rumore. I canali in questione, tuttavia, non possono essere finemente descritti tramite la posizione geografica delle antenne, in quanto nel loro funzionamento si limitano ad applicare il comportamento di un canale generico, in modo tale che l'ouptut prodotto sia coerente con quanto statisticamente misurabile in una situazione reale non meglio specificata. Per superare questo scoglio è stato necessario implementare un nuovo metodo di simulazione.
Lo scenario tipo sulla base del quale è stato configurato il canale di comunicazione è rappresentato in figura 5.3. È prevista la presenza di un trasmettitore (tx) e un ricevitore (rx), entrambi dispongono di un array in cui sia il numero di antenne che la distanza tra ciascuna di esse (Δ_{tx} e Δ_{rx}) è configurabile. Il centro dell'array del trasmettitore è situato alle coordinate (0,0) del piano cartesiano, mentre il centro dell'array del ricevitore è identificato dalla distanza D e dall'angolo θ rispetto alla posizione del trasmettitore. Andando a calcolare le coordinate x,y nel piano di tutte le antenne, è quindi possibile

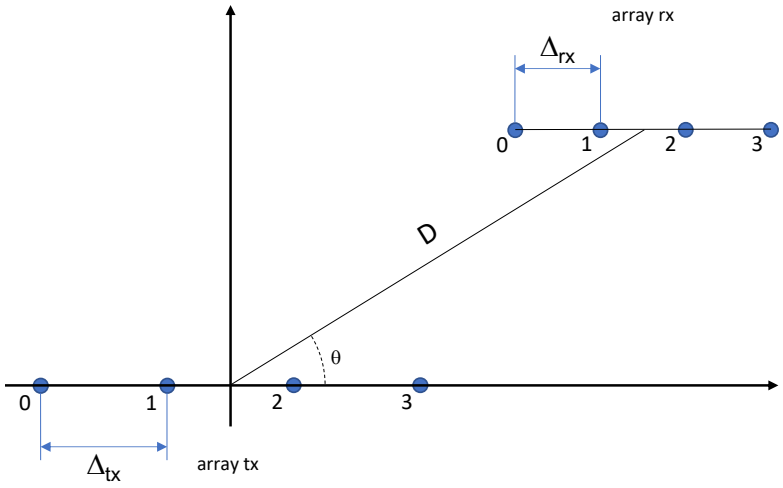

Figura 5.3: Disposizione delle antenne sul piano cartesiano nel canale simulato

determinare, per ciascuna antenna tx, la distanza relativa di ciascuna antenna rx.
Consideriamo ora un generico segnale nel dominio del tempo $s_{tx}(t)$ centrato alla frequenza f_0:

$$s_{tx}(t) = 2\Re\left[c_{tx}(t)\exp(j2\pi f_0 t)\right]$$

dove l'inviluppo complesso c è:

$$c_{tx}(t) = \int_{-\infty}^{+\infty} C_{tx}(f) e^{j2\pi ft} df$$

Durante la sua propagazione verso il ricevitore, il segnale accumula uno ritardo di fase determinato da zf/c, dove z è la distanza percorsa e c la velocità di propagazione (Velocità della luce).
Fissata una distanza z, il segnale può quindi essere scritto come

$$s_{rx}(t, z) = 2\Re\left[c_{tx}(t - z/c)\exp(j2\pi f_0(t - z/c))\right] \tag{5.1}$$

Per calcolare il segnale effettivamente ricevuto su ogni antenna del ricevitore, è necessario sommarvi il segnale proveniente da tutte le n antenne usate dal trasmettitore (eq. 5.1), ciascuno con la propria distanza $z_{j,k}$ dove j rappresenta la j-sima antenna del trasmettitore e k la k-sima antenna del ricevitore.

$$c_{rx,k}(t) = \sum_{j=0}^{3} c_{tx}(t - z_{j,k}/c)\exp\left[-j2\pi f_0 z_{j,k}/c\right] \tag{5.2}$$

Analizzando unicamente i ritardi relativi di ciascun segnale $\Delta t_{j,k}$

$$\Delta t_{j,k} = \left(z_{j,k} - \min_{j,k} z_{j,k}\right)/c \tag{5.3}$$

l'equazione 5.2 diventa:

$$c_{rx,k}(t) = \sum_{j=0}^{3} c_{tx}(t - \Delta t_{j,k})\exp\left[-j2\pi f_0 \Delta t_{j,k}\right] \tag{5.4}$$

e rappresenta, per ogni antenna al ricevitore, il segnale nel dominio del tempo relativo all'NDP inviato da ciascuna antenna del trasmettitore.

Generazione delle CSI al beamformee e compressione in angoli Le CSI sono generate tramite alcune funzioni Matlab del WLAN Toolbox, che prima vengono utilizzate anche per convertire nel dominio delle frequenze il segnale ricevuto, e successivamente per rimuovere l'effetto dovuto al CSD dal canale misurato.
Dopo aver estratto le feedback matrix utilizzando la Singular Value Decomposition, si utilizza un'implementazione del metodo di compressione e quantizzazione (in questo caso sempre proveniente dal WLAN Toolbox) per ottenere tutti gli angoli corrispondenti alle matrici, partendo dalla matrice V. Gli angoli vengono salvati in un file .mat, sotto forma di una matrice che segue lo stesso ordine di come gli angoli sono inseriti all'interno del report.

Simulazione della comunicazione "beamformata"

A questo punto, gli angoli da inserire nel Report sono stati finalmente ricavati. Con lo stesso script, è anche possibile sfruttarli per simulare la comunicazione di data con la tecnica del beamforming. Per fare ciò si utilizza la funzione simmetrica alla compressione, che dati gli angoli in input esegue la de-quantizzazione e successivamente la decompressione, restituendo di nuovo la medesima matrice V che il trasmettitore userà per sterzare la trasmissione. È interessante analizzare l'effetto della quantizzazione su V in figura 5.4, si può notare come, sebbene l'andamento del modulo sia catturato correttamente, vi sia una perdita di risoluzione. Si ottiene un risultato analogo anche con il grafico della fase del numero complesso. Nelle figure 5.5 e 5.6 sono rispettivamente mostrate le costella-

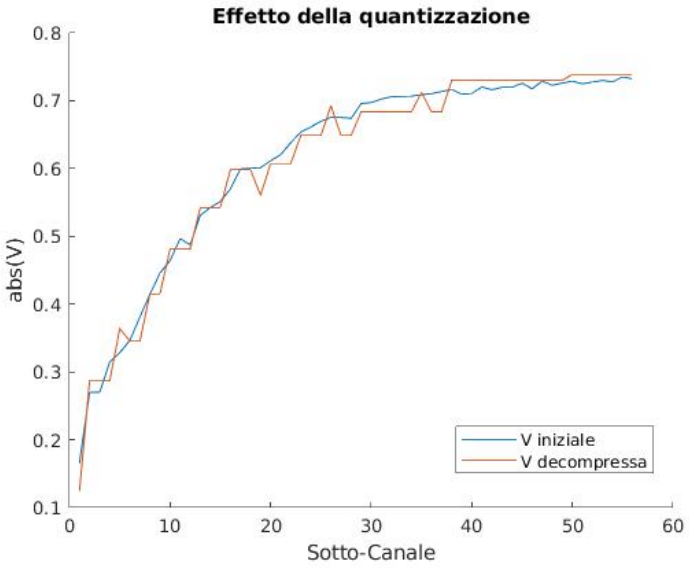

Figura 5.4: Effetto della quantizzazione sulle 56 matrici V_k, una per ogni sotto-canale, prendendo come esempio la prima riga e la prima colonna, cioè il contributo della prima antenna in trasmissione al primo stream spaziale

zioni 16-QAM per una simulazione di due stream spaziali beamformata ed una non. Le potenze del segnale misurate al ricevitore sono, nel primo caso, di $2.07W$ per il primo stream e $0.45W$ per il secondo, mentre nel caso non beamformato sono $0.9W$ e $0.57W$. Come si può notare sia dalle potenze misurate che da un'analisi grafica delle figure, per via dell'ordinamento eseguito nella procedura dell'SVD, il primo stream del beamforming è prioritario e viene sempre ottimizzato maggiormente, portando ad una varianza inferiore nella costellazione (figura 5.5 - blu), mentre nel caso privo del beamforming sia la varianza che la potenza misurata cadono più o meno nello stesso intervallo. Nel caso specifico dell'esempio mostrato, il secondo stream non ha ottenuto alcun vantaggio nel passaggio al beamforming rispetto al caso base.

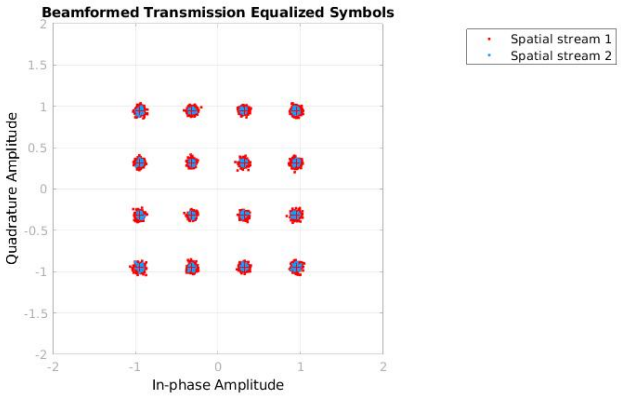

Figura 5.5: Costellazione per una trasmissione X con il beamforming. I punti di colore rosso rappresentano le IQ relative allo stream 1, i punti di colore blu quelle relative allo stream 2. Si noti come la varianza dei punti blu sia molto minore rispetto a quella dei punti rossi

Limitazioni e commenti alla simulazione di una comunicazione Wi-Fi via software

- È in grado di simulare comunicazioni con qualsiasi configurazione mimo, fino a 8 $\times$ 8 : 8.
- L'ampiezza del canale può variare da 20 a 160Mhz.
- Si assume che le antenne di un dato array siano necessariamente equi spaziate, nonostante questa possa sembrare una scelta guidata dal buonsenso, per via di vincoli costruttivi o regolatori, spesso vari dispositivi commerciali non hanno tutte le antenne distribuite parallelamente, oppure hanno una o più antenne "interne", posizionate in una logica diversa dal resto dell'array.
- La simulazione del canale è deterministica e non introduce la propagazione degli stream di dati su linee diverse dalla line-of-sight. Questo risulta essere un problema cruciale in quanto è fondamentale avere più linee di propagazione diverse, per poter applicare il beamforming con maggiore successo.

5.2.2 Generazione degli angoli a partire da una CSI

Questa modalità è di fatto un sottoinsieme di quanto avviene con la simulazione completa del canale: una CSI generata da una qualsiasi sorgente può essere trattata esattamente come avviene con le CSI generate dalla simulazione. Una singola CSI per uno specifico sotto-canale tra due antenne è rappresentata da un numero complesso, quindi la dimensione della CSI completa dipende dal numero di sotto-canali (64 per 20Mhz di ampiezza), dal numero di antenne al trasmettitore e dal numero di antenne al ricevitore. Come nel

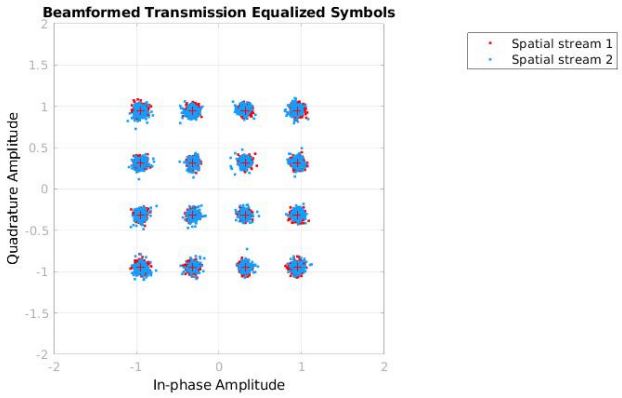

Figura 5.6: Costellazione per una trasmissione X senza il beamforming. I punti di colore rosso rappresentano le IQ relative allo stream 1, i punti di colore blu quelle relative allo stream 2.

caso precedente, le CSI vengono convertite in angoli dalla relativa funzione matlab, e sono successivamente inseribili in un report.

5.2.3 Generazione degli angoli a partire dalla loro formulazione prevista dallo standard

In questo caso non è necessario utilizzare alcun software specifico, ma bisogna riuscire a decodificare e dare un significato deterministico a ciascun passaggio operato durante la compressione. Come vedremo nel capitolo successivo, nel caso di una trasmissione 3×1, la procedura assume un'intepretazione geometrica più accessibile, sulla quale è possibile fare inferenza per determinare direttamente il valore degli angoli sulla base del risultato desiderato.

Capitolo 6

Raccolta e presentazione dei risultati

Nella piattaforma adottata per il test, è stato utilizzato un router Asus rt-ac86u come Beamformer. Il router in questione supporta lo standard 802.11ac ed è dotato di quattro antenne, tre delle quali sono esterne (figura 6.1).

Come beamformee sono stati utilizzati, in sequenza, un Raspberry 3B+, un analogo

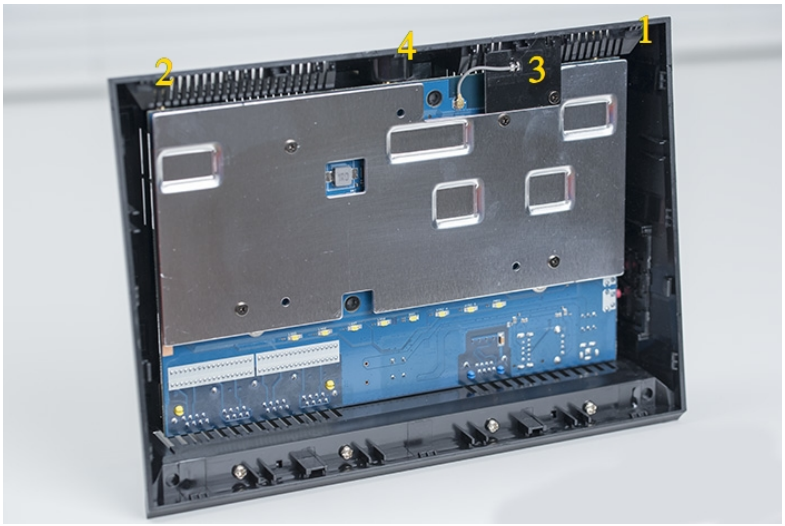

Figura 6.1: Vista frontale della board del Router Asus rt-ac86u con indicate le quattro radio chain, di cui una interna

Asus rt-ac86u e uno smartphone LG Nexus 5. Infine, per analizzare le CSI prodotte dal trasmettitore una volta effettuato il beamforming, è stato utilizzato un ulteriore router Asus ax86u, aderente in questo caso al più recente standard 802.11ax. Con tutti e tre i sistemi è stato possibile inviare un report fornito in input dall'utente, anche

se per fare ciò è stato chiaramente necessario introdurre un'opportuna customizzazione software per renderli in grado di effettuarne il processamento. Oltre al dimostrare il funzionamento dell'iniezione su più dispositivi, la varietà messa in campo è servita per testare più configurazioni di antenne, che generano un sistema 4x4 quando i due router Asus sono in uso, e un sistema 3x1 con il raspberry e il Nexus, i quali aderiscono a loro volta allo standard 802.11ac e sono dotati di un'unica antenna. Nell'interfacciamento con questi ultimi, pare che sia necessario che il router Asus disabiliti un'antenna, come è possibile constatare nel campo VHT MIMO Control (visionabile in figura 6.2 e spiegato nel paragrafo 4.1.3) di un qualsiasi report inviato dal Nexus, riducendo così il sistema ad un 3×1. Il vantaggio derivato da questo comportamento, è che la procedura per

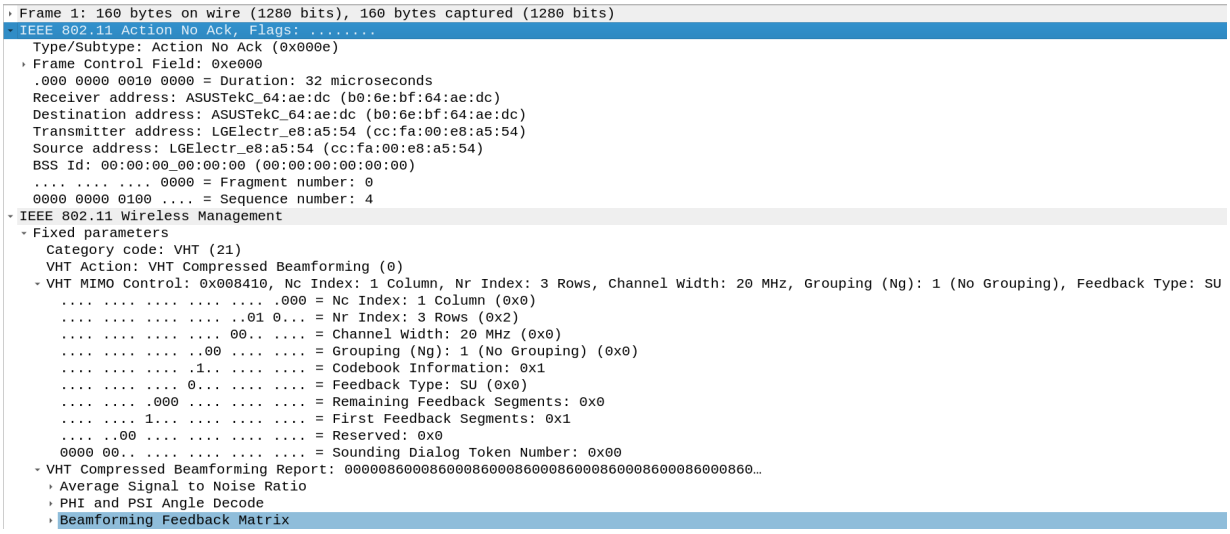

Figura 6.2: Esempio di un Compressed report inviato dal Nexus. Si tratta di un report SU per tre antenne di trasmissione ed un solo stream spaziale, con un canale di ampiezza 20Mhz. Le dimensioni globali del report sono di 164 byte (ai 160 mostrati su wireshark vanno aggiunti 4 byte di FCS), compatibili con le dimensioni richieste da un report contenente quattro angoli per ogni sottocanale.

la generazione della feedback matrix, e successivamente per la derivazione degli angoli, assume un significato geometrico di più immediata interpretazione ed applicazione. In tutti i casi in cui l'antenna al ricevitore sia soltanto una, infatti, in alternativa al calcolo della matrice V usando la Singular Value Decomposition partendo dalle CSI (matrice H), è possibile usare la seguente equazione:

$$V = \frac{H^H}{\sqrt{HH^H}} \tag{6.1}$$

Dove l'H all'esponente indica l'operatore Hermitiano (Matrice coniugata trasposta). Ancora, considerando la V ricavata nel caso del nexus per un singolo sotto-canale: $V =$

$[v_1 v_2 v_3]^T$, dove ogni v è un numero complesso che rappresenta un'antenna in trasmissione, i 4 angoli ricavabili con la decompressione sono:

$$\begin{aligned} \phi_{11} &= \angle(v_1) - \angle(v_2), \\ \phi_{21} &= \angle(v_2) - \angle(v_3), \\ \psi_{21} &= \arctan\left(\frac{|v_2|}{|v_1|}\right), \\ \psi_{31} &= \arctan\left(\sqrt{\frac{|v_3|^2}{|v_1|^2 + |v_2|^2}}\right). \end{aligned} \tag{6.2}$$

6.1 Configurazione dei dispositivi

Configurazione del Nexus Per permettere al Nexus 5 di iniettare i report inseriti dall'utente, dopo la richiesta che il beamformer comunica attraverso un NDP Announcement e poi un NDP, è stato necessario utilizzare il framework *Nexmon* [20], il quale permette di accedere e gestire direttamente i chip Wi-Fi Broadcom/Cypress utilizzati in numerosi dispositivi commerciali aderenti agli standard 802.11. Oltre a permettere di iniettare trame dallo spazio utente alla radio, il framework può essere utilizzato anche per monitorare tutti i pacchetti che transitano nella rete, estrarre CSI ed utilizzare il chip come una software defined radio. Il chip specifico utilizzato dal Nexus è denominato *bcm4339* ed è direttamente supportato dall'utility. Per poter iniettare le trame create con matlab, è necessario modificare il microcode contenuto nel firmware del chip, usando le utility offerte da Nexmon e connettendo il Nexus ad un calcolatore tramite l'interfaccia *adb*[1], grazie alla quale sarà poi possibile lanciare tutti i comandi. La modifica apportata, entra in funzione nel momento in cui il Nexus riceve il NDP e sta per inviare il report calcolato. A questo punto, infatti, invece di utilizzare l'engine interno per restituire un report genuino, è stata indicata un'area libera nella shared memory dalla quale attingere al report caricato dall'utente. Quando questa modifica è attiva, ogni volta che il Nexus riceve la richiesta di un report, sarà inviato sempre e comunque quello presente nella shared memory, fornendo una configurazione stabile sulla quale è possibile effettuare le dovute misurazioni.

Configurazione del Raspberry La configurazione del Raspberry model 3B+ è equivalente a quella del Nexus. Il chip utilizzato da questo dispositivo è denominato *bcm43455c0* ed è a sua volta supportato dal framework Nexmon. Una volta constatata la capacità del dispositivo di iniettare i frame relativi ad un beamforming report, non è stato ritenuto opportuno condurre ulteriori test considerando che la configurazione del canale utilizzato risulta essere equivalente a quella del Nexus.

[1] Android Debug Bridge, è un'interfaccia a linea di comando per dispositivi android, che fornisce accesso ad una shell linux

Configurazione dei Router Asus La configurazione dei router Asus ha seguito più strade parallele in base alla funzionalità sfruttata. Come anticipato, il beamformer a cui viene modificato il diagramma di radiazione non necessita di alcuna modifica. Il router utilizzato per iniettare i compressed report, con il chip *bcm4366c0*, è stato patchato a sua volta usando il framework nexmon. Infine, il router utilizzato per catturare le CSI inviate dal beamformer è stato patchato con un tool per l'estrazione delle CSI, rilasciato ancora una volta da Nexmon [15].

6.1.1 Configurazione delle antenne al trasmettitore nel caso 3x1

Per poter determinare quale delle quattro antenne presenti nel trasmettitore Asus viene disattivata quando il destinatario della comunicazione è il Nexus (Mimo 3x1 verso un dispositivo mono-antenna), è stata utilizzata una USRP (*Universal Software Radio Peripheral*, SDR commercializzata da *Ettus Research*) B210, con la quale abbiamo raccolto con un ratio di 20MS la forma d'onda generata da tutti i trasmettitori connessi ad uno specifico canale a 5Ghz (il 157, di ampiezza 20Mhz e con frequenza centrale pari a 5785Mhz) in un dato momento, assicurandoci che la banda in questione fosse occupata esclusivamente da uno scambio di dati tra il router Asus ed il Nexus, mentre era attiva la configurazione del beamforming. Così facendo, è stato possibile visualizzare graficamente, in figura 6.3, lo scambio degli NDPA, NDP e Compressed Report tra il beamformer ed il beamformee. Per processare i dati in questione, è stato utilizzato uno script di Matlab [18] in grado di decodificare i campi a livello fisico di un generico pacchetto 802.11ac.

A questo punto, analizzando più nel dettaglio il frame relativo al NDP (figura 6.4), è stato possibile raccogliere nel campo VHT-LTF le informazioni sul canale MIMO in uso e quindi le corrispondenti CSI prodotte da ciascuno stream spaziale. Il caso base, dove tutte e tre le antenne sono normalmente in funzione è mostrato in figura 6.5(a). La procedura in questione è stata iterata più volte rimuovendo fisicamente un'antenna dal router Asus per ogni iterazione e lasciando tutte le altre in una condizione uguale al caso base. In figura 6.5(b) è mostrato a titolo d'esempio il caso in cui è stata rimossa l'antenna 1. Rimuovendo l'antenna esterna centrale (si veda la figura 6.1 del router come riferimento), che d'ora in poi chiameremo antenna 4, è stato possibile ottenere una misura delle CSI equivalente al caso base, deduciamo quindi che il router ac86u utilizzi uno schema di ordinamento particolare per le antenne (da sinistra a destra: 2, 4, 3-interna, 1), e che anziché implementare un array parallelo per le comunicazioni MIMO 3×1 usando tutte le antenne esterne, si limita a disabilitare l'antenna centrale.

A questo punto, abbiamo utilizzato uno specifico supporto (figura 6.6), sul quale sono state montate tre antenne parallele ed equi-spaziate che sono poi state collegate alle corrispettive antenne usate dall'Asus, in modo tale che fossero disposte da sinistra a destra secondo l'ordine appena determinato, ed abbiamo testato un'ulteriore trasmissione, visibile in figura 6.7. In questo caso, utilizzando per tutte e tre lo stesso tipo di antenna, anche l'ampiezza misurata sull'antenna 3, che inizialmente era interna, è paragonabile alle altre. Un secondo effetto è che cambiando le antenne anche la dinamica delle CSI

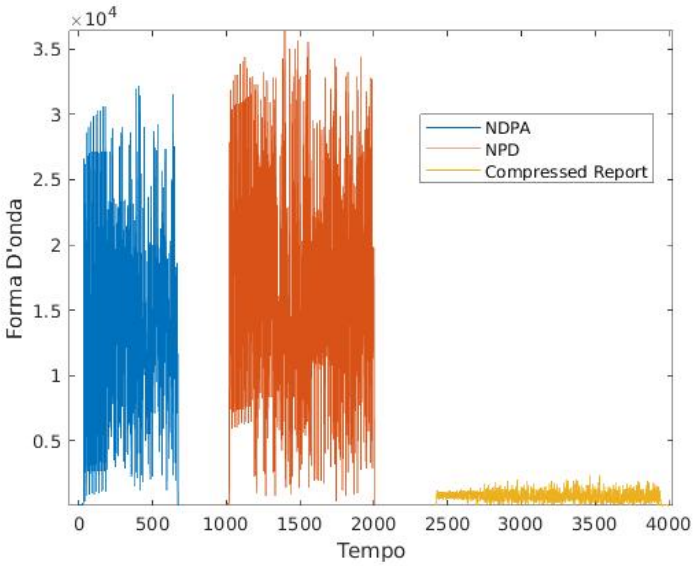

Figura 6.3: Procedura di sounding catturata tramite l'USRP. Gli NDPA ed NDP inviati dal router Asus risultano graficamente molto più ampi rispetto al Report inviato dal Nexus in quanto l'USRP era posizionato a fianco dell'Asus durante la misurazione.

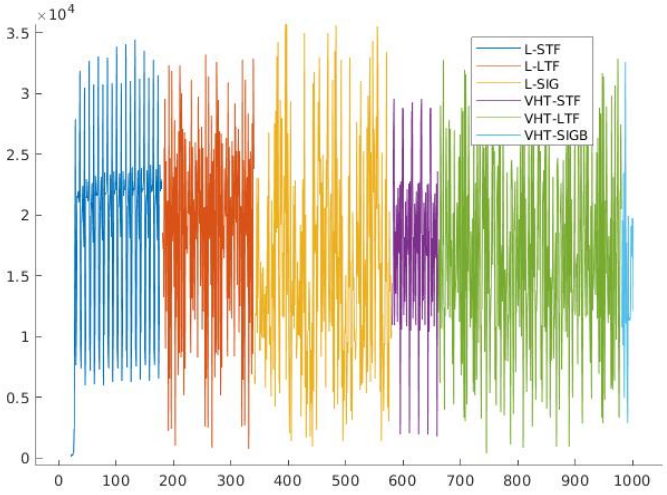

Figura 6.4: Dettaglio del Null Data Packet catturato con l'USRP in cui sono evidenziati tutti i campi a livello fisico presentati in figura 3.5. Il frame termina con il campo VHT SIG-B, senza alcun valore nel campo data

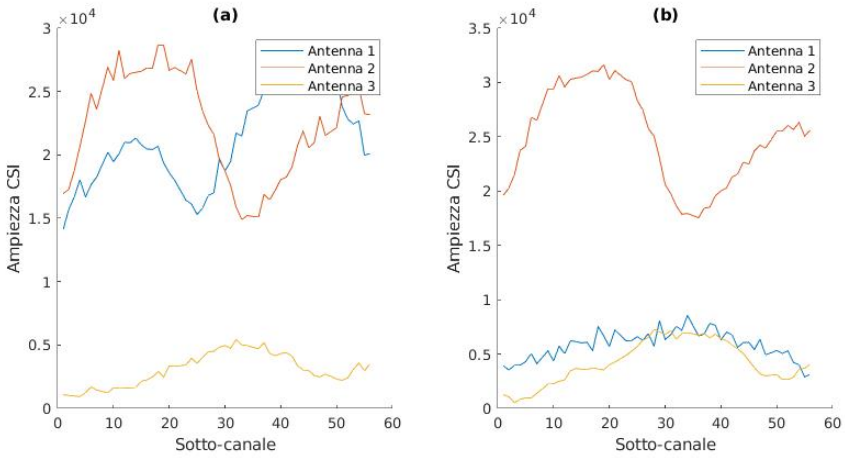

Figura 6.5: Le CSI relative al NDP catturato dall'USRP per ciascuno dei 56 sotto-canali del canale 157 da 20Mhz in un MIMO 3x1. La CSI misurata sull'antenna 3 è più bassa delle altre in quanto si tratta dell'antenna interna al router.
(a) Caso standard. (b) Caso in cui l'antenna uno è stata rimossa, l'ampiezza della csi diventa simile a quella naturalmente ottenuta con l'antenna interna

misurate è necessariamente diversa rispetto a quanto ottenuto negli altri test. Con questo nuovo posizionamento, è stato possibile verificare, in un contesto non beamformato, quindi dovuto solamente ai requisiti fisici di progettazione delle radio chain all'interno del router, come ciascuno stream fosse sfasato rispetto agli altri. Per ottenere un risultato più preciso, inoltre, in una seconda misurazione le tre antenne sono state sostituite da tre cavi coassiali che convergevano fisicamente verso L'ingresso della singola antenna usata sull'USRP utilizzando tre muxer 2-in-1 (figura 6.8), in modo da eliminare le variazioni di fase dovute alla trasmissione nell'aria. La porta inutilizzata di uno dei muxer è stata chiusa su una resistenza da 50ohm per evitare problemi di cattivo accoppiamento di impedenza. La misurazione delle fasi per ciascuna CSI ottenuta è presentata in figura 6.9, ed evidenzia come, seppur tra ciascun sotto-canale vi sia una variazione, la differenza di fase venga preservata tra tutte le antenne, inclusa quella che originariamente era interna. In particolare, calcolando la fase media su tutti i sotto-canali rispetto all'antenna 1, risulta uguale a 2.67 sull'antenna 2, e -2.30 sulla 3.

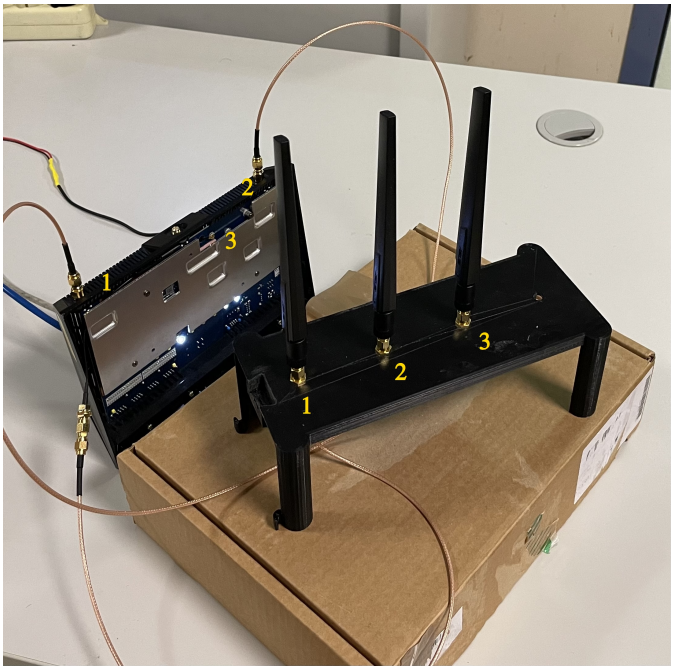

Figura 6.6: Trasformazione delle tre antenne usate dall'Asus rt86u nelle comunicazioni 3x1 in un array parallelo

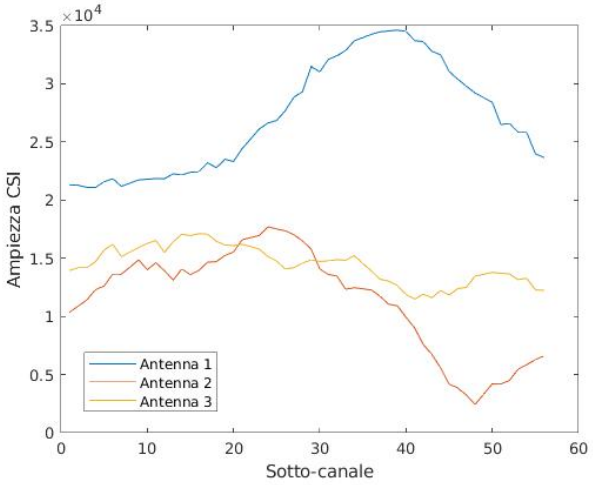

Figura 6.7: Misura delle CSI di un MIMO 3x1 con l'USRP quanto le tre antenne al trasmettitore sono state rese parallele, si noti come l'antenna 3 abbia un'ampiezza simile alle altre due antenne

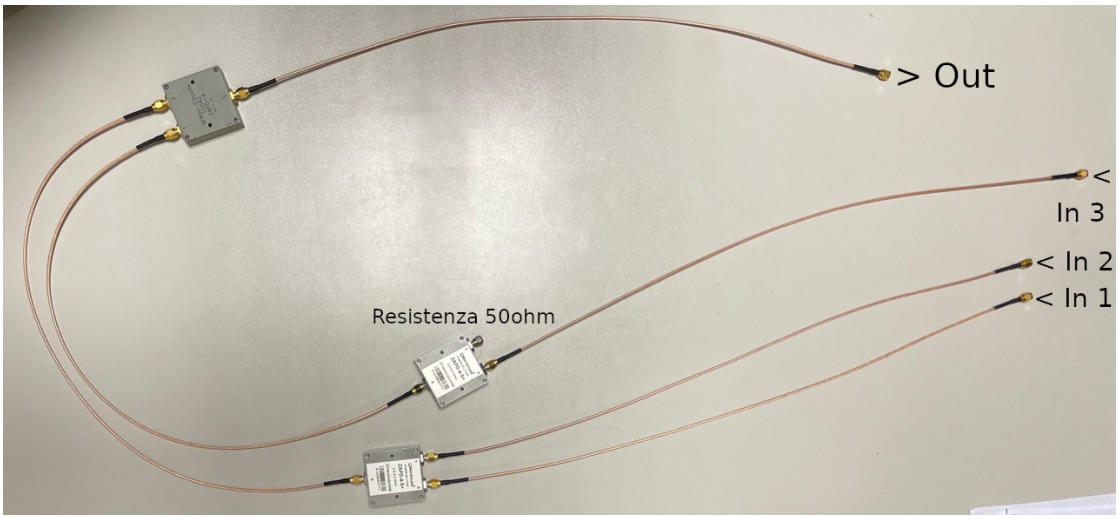

Figura 6.8: Connessione fisica tra le tre antenne del trasmettitore (In 1, 2 e 3) e l'antenna dell'USRP (Out) utilizzando cavi coassiali e muxer 2-in-1. All'estremita non utilizzata di uno dei due muxer è presente una resistenza da 50ohm

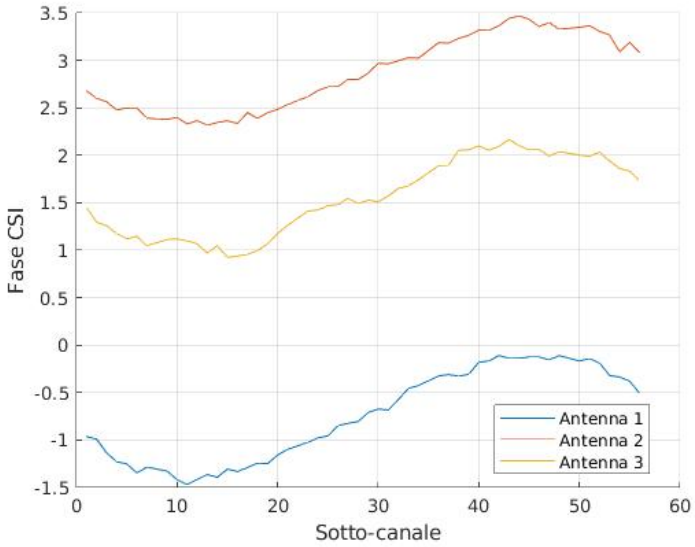

Figura 6.9: Misura delle fasi delle CSI di un MIMO 3x1 quanto le tre antenne al trasmettitore sono state collegate direttamente all'USRP, per determinare come ciascuna antenna sfasa il segnale senza beamforming

6.2 Risultati raccolti

Come referenza per il confronto con i prossimi risultati, nella figura 6.10 sono mostrate le misurazioni delle CSI trasmesse dal router Asus quando la procedura del beamforming avviene normalmente, senza che il report sia manipolato dall'utente. Chiaramente, il grafico ottenuto con questo test dipende fortemente dalle posizioni reciproche tra il beamformer ed il beamformee, che influenzano la generazione del report, e dalle posizioni tra il beamformer ed il router usato per catturare le CSI, da cui dipende il percorso delle onde radio misurate.
In condizioni ideali, la curva prodotta dovrebbe essere lineare e priva di sbalzi. Il valore corrispondente al sotto-canale centrale è anche il valore minimo misurato, in quanto questo, per esigenze dovute all'OFDM, non viene utilizzato per trasmettere data.

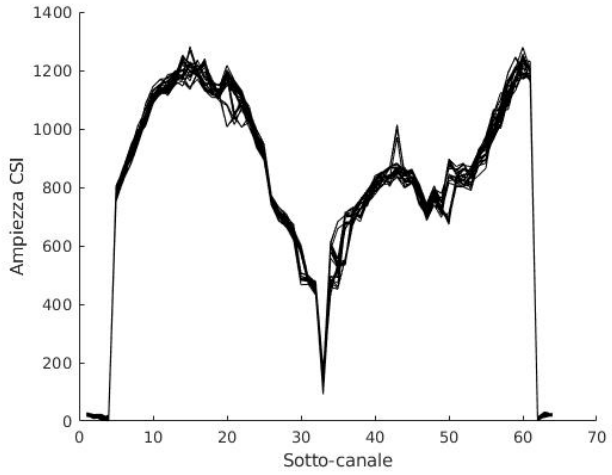

Figura 6.10: Ampiezza delle CSI misurate quando il beamforming è in funzione normalmente

Risultati utilizzando un report casuale Impostare il beamforming con un report nel quale gli angoli sono stati inseriti con dei valori completamente casuali, provoca una notevole distorsione delle CSI misurate al ricevitore (figura 6.11). Risultati di questo tipo sono stati utili per verificare se il report fabbricato tramite gli script introdotti in questa tesi fossero realmente utilizzati dal beamformer: nel caso in cui il report dovesse contenere delle informazioni incompatibili con quanto previsto dallo standard è possibile che il trasmettitore lo ignori completamente e continui ad utilizzare l'ultimo report precedentemente ricevuto, o passi ad una comunicazione che non utilizza beamforming esplicito.

Test con i risultati prodotti dal simulatore del canale Utilizzando gli angoli prodotti dal software con la simulazione del canale MIMO 3x1 per inviare un report

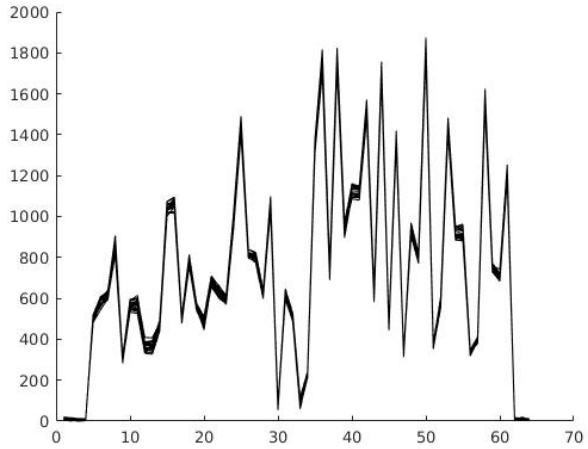

Figura 6.11: Ampiezza delle CSI misurate quando il beamforming è stato impostato con valori completamente casuali

al beamforming, si ottiene durante la comunicazione una misurazione delle CSI ancora abbastanza rumorosa (figura 6.12). Ciò è probabilmente dovuto al fatto che la geometria utilizzata all'interno del simulatore non combacia con quanto sperimentabile nella realtà: nel caso specifico preso in esame, di fatti, l'array di antenne usato dal beamformer presenta un'antenna interna che non è parallela alle altre, inoltre le antenne non sono utilizzate in sequenza ma secondo un ordinamento diverso. Il simulatore, invece, considera tre antenne in sequenza una parallela all'altra, di conseguenza, anche la distanza tra ciascuna antenna non è quella corretta.

Provando a trasmettere lo stesso report quando è in uso il supporto mostrato in figura 6.6, che uniforma la geometria dell'array del trasmettitore reale con quella presentata nel simulatore, si ottiene una misurazione più coerente con l'aspettativa, in figura 6.13.

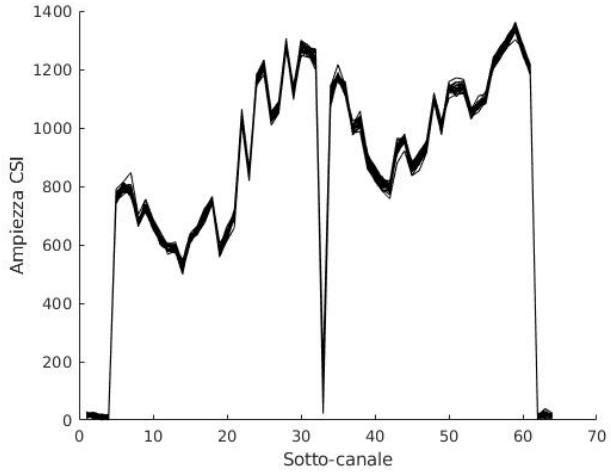

Figura 6.12: Ampiezza delle CSI misurate quando il beamforming è stato impostato con gli angoli ottenuti dalla simulazione, configurata con un array al trasmettitore diverso dalla realtà

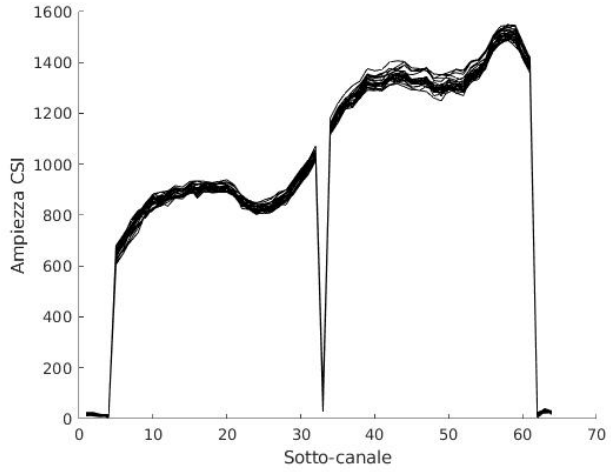

Figura 6.13: Ampiezza delle CSI misurate quando il beamforming è stato impostato con gli angoli ottenuti dalla simulazione, configurata con un array al trasmettitore equivalente realtà

6.2.1 Test con i report prodotti dal simulatore in campo aperto

Il test finale è stato eseguito per verificare come varia la potenza del segnale ricevuto su un dispositivo al variare dell'angolo impostato nel simulatore per la trasmissione del beamforming (figura 5.3). Se lo script viene eseguito correttamente, infatti, ci si può aspettare che la potenza ricevuta sia massima quando l'angolo del beam impostato via software corrisponde alla direzione reale tra il trasmettitore ed il ricevitore, e che più ci si allontani dal valore ideale più la potenza ricevuta decresca. Per stabilizzare le condizioni, il test è stato eseguito in un ambiente il più statico possibile e sufficientemente ampio da minimizzare le riflessioni con le pareti circostanti (idealmente, il test dovrebbe essere svolto in campo aperto). In figura 6.14, è stata schematizzata la disposizione dei router utilizzati durante l'esperimento, mentre in figura 6.15 si può vedere la disposizione reale.
Il beamformer ed il beamformee sono rispettivamente il router Asus ac86u le cui tre

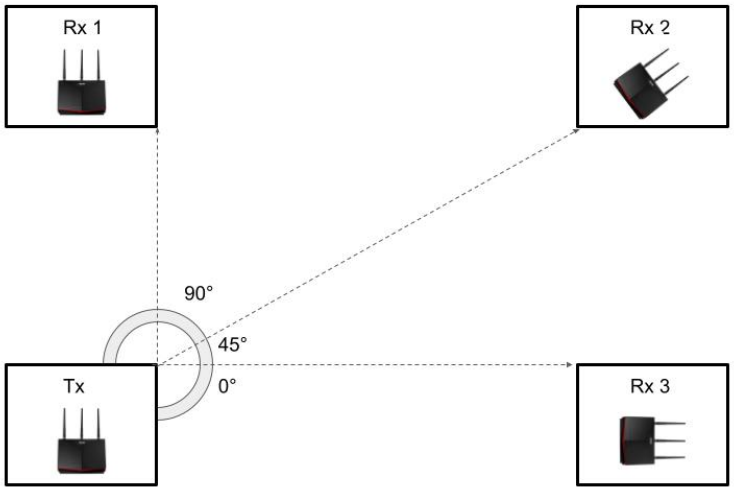

Figura 6.14: Disposizione a forma di quadrato dei quattro router usata nell'esperimento in campo aperto. Ciascun router è stato idealmente posizionato su uno dei vertici

l

antenne usate per le comunicazioni MIMO 3x1 sono state rese parallele come in figura 6.6 ed il Nexus 5 che non compare nella rappresentazione grafica perché viene usato solo per trasmettere i report. Per raccogliere le CSI sono stati utilizzati tre router Asus ax86u configurati tutti allo stesso modo e disposti in tre direzioni diverse, in modo tale che uno fosse posizionato a 0° rispetto al trasmettitore, uno a 45 e uno a 90.
L'esperimento è consistito nell'inviare, tramite il compressed report del Nexus, 90 diverse configurazioni del Beamforming simulato, in modo tale da direzionare il beam verso

Figura 6.15: Fotografia con la disposizione a forma di quadrato dei quattro router usata nell'esperimento in campo aperto, nell'atrio dell'Università degli studi di Brescia. A fianco del Beamformer Tx è possibile notare anche il Nexus 5 utilizzato come Iniettore, collegato a un computer desktop tramite l'interfaccia ADB e l'USRP utilizzata per misurare le fasi di ciascuna antenna.

tutti gli angoli compresi tra 0 e 90 gradi. Per ogni nuovo report inviato, ciascuno dei tre router ax ha eseguito una misurazione delle CSI, grazie alla quale è anche possibile estrarre la potenza del segnale ricevuto. Infine, è stata graficamente mostrata la variazione di potenza misurata su ciascuna antenna di ciascun ricevitore. Prima di procedere con il test vero e proprio, è stata eseguita una nuova misurazione del ritardo in fase tra ciascuna radio chain del trasmettitore tramite l'USRP. I valori ottenuti, a distanza di giorni dalla prima misurazione e in un'ambiente completamente diverso, sono risultati coerenti con le misurazioni precedenti. Inoltre, per una maggiore aderenza alla realtà, il simulatore del beamforming è stato configurato secondo tutte le proprietà del canale realmente in uso: un MIMO 3x1 centrato sulla banda a 5785 Mhz (canale 157), con la distanza tra le antenne nell'array del trasmettitore pari a 5.8cm e uno sfasamento di -2.5 tra la prima e la seconda antenna, e di +2.3 tra la prima e la terza. Le potenze misurate sono indicate in figura 6.16. Il valore mostrato è in dB. Confrontando il valore di potenza massimo misurato per ciascuna antenna con il valore minimo, si ottiene che il guadagno tra l'angolo peggiore e l'angolo migliore è nell'intorno di 15dB. Una variabilità di questo tipo, è sicuramente oltre le potenzialità di un sistema di beamforming con tre antenne al trasmettitore, tuttavia bisogna considerare che la mancanza della componente multipath al simulatore, e di contro la sua presenza nell'esperimento reale nonostante il campo

aperto, potrebbe verosimilmente aver configurato dei beam particolarmente variabili. Lo

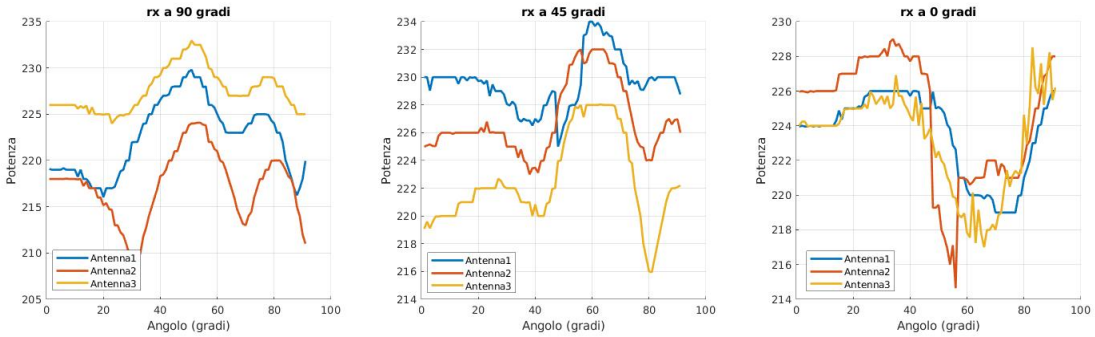

Figura 6.16: Potenze misurate sui ricevitori posizionati a 90 (Rx 1), 45 (Rx 2) e 0 (Rx 3) gradi. Per ciascun ricevitore sono state mostrate tre antenne su quattro, in quanto è stata esclusa la misurazione proveniente dall'antenna interna

stesso esperimento è stato svolto in ambiente completamente simulato su Matlab, ed ha prodotto i risultati in figura 6.17.

Effettuando un confronto tra le misurazioni reali e quelle nel simulatore, si riscontra una

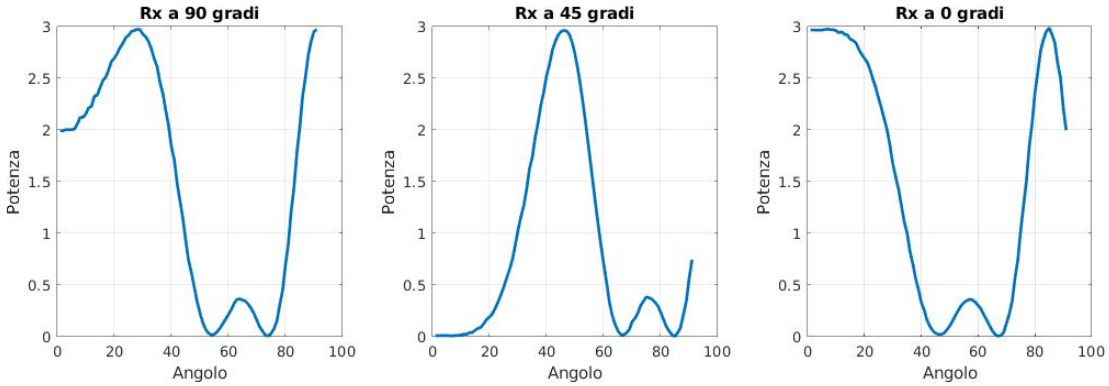

Figura 6.17: Potenze misurate sui ricevitori posizionati a 90, 45 e 0 gradi nel simulatore. Per ciascun ricevitore è mostrata un'unica antenna in quanto il simulatore era configurato con un MIMO 3x1

dinamica abbastanza differente. Innanzitutto, il simulatore, avendo dei canali deterministici senza multipath, coglie perfettamente il massimo della potenza ricevuta quando l'angolo configurato corrisponde esattamente a quello dove è posizionato il ricevitore. Nel caso reale, invece, nonostante permanga una certa continuità nella misurazione della potenza tra angoli adiacenti, cioè il simulatore è effettivamente in grado di configurare dei beam focalizzati in alcune direzioni, i picchi di potenza misurati non sono in corrispondenza dell'angolo a cui il ricevitore è stato posizionato. Considerando il caso del

Rx 1 posizionato a 90 gradi, sono stati trovati una serie di picchi posizionati a livelli diversi intorno ai 50 e agli 80 gradi. Questo aspetto è dovuto al fatto che in realtà, per motivi costruttivi, durante la configurazione del beamforming non viene generato esclusivamente un unico lobo principale verso la direzione specifica, ma per effetto della steering matrix applicata alle radio chain si generano anche altri lobi secondari che puntano in più direzioni diverse. Nel caso del Rx 3 posizionato a 0 gradi, la misura delle potenze è nettamente più rumorosa rispetto agli altri due. Il motivo è che la configurazione del beamforming è meno efficace quando la direzione del beam è parallelo all'array di antenne del trasmettitore.

Capitolo 7

Conclusioni

In questa tesi, abbiamo studiato il funzionamento e la configurazione del Beamforming su dispositivi aderenti allo standard IEEE 802.11. In particolare, abbiamo implementato una procedura per il controllo del diagramma di radiazione di un trasmettitore attraverso la ricezione di un Compressed Beamforming report opportunamente configurato dall'utente. Per lo scopo prefissato, è stato inoltre necessario sviluppare un iniettore che sia in grado di intervenire mebtre il firmware del beamformee sta per inviare un compressed report, consentendo di inserire nel momento più opportuno il frame costruito dall'utente al posto del report genuinamente calcolato dal beamformee. Questo particolare iniettore, necessita di un profondo lavoro di reverse engineering sullo specifico firmware usato da ciascun beamformee, per identificare e modificare le aree di memoria e del micro-code interessate nel processing del beamforming. Come software di supporto a tutta l'attività di costruzione del report, è stato implementato un simulatore del canale di comunicazione e del beamforming in Matlab. Infine, abbiamo verificato l'efficacia del sistema di controllo su più dispositivi beamformee commerciali ricavando con un captatore Wi-FI le CSI relative al canale di comunicazione usato dal trasmettitore, confrontandone l'andamento con quanto ricavabile durante altre trasmissioni di dati. Grazie al lavoro svolto, quindi, è ora possibile utilizzare un qualsiasi dispositivo in grado di iniettare trame Wi-Fi fornite dall'utente per manipolare e riconfigurare, durante la comunicazione, le direzioni verso cui la radiazione viene concentrata. Per quanto riguarda il simulatore, invece, sono state rilevate alcune criticità e disallineamenti rispetto ad un'implementazione reale, dovute alla mancanza di multi-path, alla presenza di un canale deterministico e all'impossibilità di inserire tutte le variabili costruttive ed ambientali che influenzano una comunicazione reale. Il software e le metodologie introdotte durante questa tesi rimangono comunque a disposizione di tutte quelle attività, scientifiche e non, che includono lo studio e la manipolazione delle CSI e della radiazione emessa da un beamformer.

Bibliografia

[1] IEEE Std 802.11-2016, IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[2] Matthew S. Gast, 802.11ac: A Survival Guide, O'Reilly Media, Inc., 2013.

[3] Matthew S. Gast, 802.11 Wireless Networks: The Definitive Guide, O'Reilly Media, Inc., 2005.

[4] P.Patil; M.R.Patil; S.Itraj; U.L.Bomble, A Review on MIMO OFDM Technology Basics and More, 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC).

[5] C.Yuen; S.Sun, Beamforming matrix quantization with variable feedback rate, 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications.

[6] H.Yu, T.Kim Beamforming Transmission in IEEE 802.11ac under Time-Varying Channels, 2014.

[7] Gentner, Christian, Avram, Diana, "WiFi-RTT-SLAM: Simultaneously Estimating the Positions of Mobile Devices and WiFi-RTT Access Points," Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021), St. Louis, Missouri, September 2021, pp. 3142-3148.

[8] Bo Tan, Kevin Chetty, and Kyle Jamieson. Thrumapper: Through-wall building tomography with a single mapping robot. In Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications, pages 1–6, 2017.

[9] Ma, Yongsen and Zhou, Gang and Wang, Shuangquan, WiFi Sensing with Channel State Information: A Survey. 2019

[10] Marco Cominelli, Francesco Gringoli, Renato Lo Cigno, AntiSense: Standard-compliant CSI obfuscation against unauthorized Wi-Fi sensing, Computer Communications, Volume 185, 2022, Pages 92-103.

[11] Marco Cominelli, Felix Kosterhon, Francesco Gringoli, Renato Lo Cigno, Arash Asadi, IEEE 802.11 CSI randomization to preserve location privacy: An empirical evaluation in different scenarios, Computer Networks, Volume 191, 2021.

[12] Vanhoef, Mathy and Piessens, Frank, Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, 2017.

[13] Steinmetzer, Daniel and Schulz, Matthias and Hollick, Matthias, Lockpicking Physical Layer Key Exchange: Weak Adversary Models Invite the Thief, 2015.

[14] Zhao, Jizhong & Xi, Wei & Han, Jinsong & Tang, Shaojie & Li, Xiangyang & Liu, Yunhao & Gong, Yihong & Zhou, Zehua. (2012). Efficient and Secure Key Extraction using CSI without Chasing down Errors.

[15] Francesco Gringoli, Matthias Schulz, Jakob Link, and Matthias Hollick. Free Your CSI: A Channel State Information Extraction Platform For Modern Wi-Fi Chipsets. In Proceedings of the 13th Workshop on Wireless Network Testbeds, Experimental evaluation & CHaracterization (WiNTECH 2019), October 2019

Sitografia

[16] ISO/IEC 7498-1:1994.
URL: https://www.iso.org/standard/20269.html.

[17] 802.11ac Transmit Beamforming.
URL: https://mathworks.com/help/wlan/ug/802-11ac-transmit-beamforming.html.

[18] Recovery Procedure for an 802.11ac Packet.
URL:https://mathworks.com/help/wlan/ug/recovery-procedure-for-an-802-11ac-packet.html

[19] 802.11ax Compressed Beamforming Packet Error Rate Simulation.
URL:https://mathworks.com/help/wlan/ug/802-11ax-compressed-beamforming-packet-error-rate-simulation.html

[20] Matthias Schulz, Daniel Wegemer and Matthias Hollick. Nexmon: The C-based Firmware Patching Framework.
URL: https://nexmon.org

[21] Nexmon CSI. URL: https://github.com/seemoo-lab/nexmon_csi

[22] CSI-MURDER. URL: https://ans.unibs.it/projects/csi-murder/

[23] DI-P2SL. URL: https://ans.unibs.it/projects/di-p2sl/