

UNIVERSITÀ DEGLI STUDI DI BOLOGNA

Corso di Laurea in Ingegneria e Scienze Informatiche

**ELABORATO DI TESI IN
VIRTUALIZZAZIONE E INTEGRAZIONE DI SISTEMI**

**Implementazione e Validazione Sperimentale del
Protocollo IEEE 802.11ai (FILS)**

Candidato:
Giuseppe Marini

Relatore:
Prof. Vittorio Ghini

Anno Accademico 2025/2026

INDICE

1. Introduzione.....	3
1.1 Contesto e motivazioni.....	4
1.2 Obiettivi del progetto.....	5
1.3 Struttura del documento.....	5
2. L'Evoluzione degli Standard IEEE 802.11.....	6
2.1 Architettura di riferimento: il modello MAC/PHY.....	7
Il livello fisico (PHY).....	7
Il livello MAC.....	8
2.2 Le origini: IEEE 802.11 legacy (1997) e 802.11b (1999).....	9
2.3 La banda da 5 GHz e OFDM: IEEE 802.11a (1999).....	10
2.4 La sintesi: IEEE 802.11g (2003).....	10
2.5 La rivoluzione MIMO: IEEE 802.11n (2009) — Wi-Fi 4.....	11
2.6 Il gigabit wireless: IEEE 802.11ac (2013) — Wi-Fi 5.....	11
2.7 L'era della densità: IEEE 802.11ax (2021) — Wi-Fi 6 e 6E.....	12
2.8 Verso il futuro: IEEE 802.11be (2024) — Wi-Fi 7.....	13
2.9 Riepilogo e motivazione per FILS.....	14
3. Protocolli di Autenticazione IEEE 802.11: Stato dell'Arte.....	15
3.1 Metodi EAP principali.....	16
EAP-TLS.....	16
EAP-PEAP.....	16
3.2 Limiti del WPA2-EAP in scenari ad alta mobilità.....	16
3.3 WPA3: evoluzione della sicurezza wireless.....	17
4. FILS — Fast Initial Link Setup (IEEE 802.11ai).....	18
4.1 FILS Discovery: ottimizzazione della scansione dei canali.....	19
4.2 Assegnazione dell'indirizzo IP durante l'associazione con FILS.....	20
4.3 Caching delle informazioni di autenticazione.....	20
4.4 Suite AKM e certificazione Wi-Fi.....	21
5. Confronto tra FILS e IEEE 802.11r (Fast Transition).....	22
5.1 Il vantaggio di FILS rispetto a 802.11r.....	22
6. Fase 1 — Implementazione dell'Access Point FILS su Fedora.....	23
6.1 Architettura del banco di test.....	24

6.2 Compilazione di hostapd con supporto FILS.....	24
6.3 Configurazione dell'Access Point.....	25
6.4 Infrastruttura DHCP e NAT.....	25
6.5 Conflitti con NetworkManager e KDE.....	26
6.6 Risultati della Fase 1.....	26
7. Fase 2 — Valutazione di OpenWrt su Raspberry Pi 4.....	26
7.1 Obiettivo e motivazioni.....	27
7.2 Problemi di connettività riscontrati.....	27
7.3 Limitazione critica: assenza di FILS in wpad-basic.....	27
7.4 Conclusioni sulla piattaforma embedded.....	27
8. Fase 3 — Benchmark FILS: Setup, Metodologia e Risultati.....	27
8.1 Setup del client di benchmark.....	28
8.2 Scoperta chiave: il ruolo della cache FILS.....	28
8.3 Evoluzione degli script di benchmark.....	28
Soluzione finale — bash + nmcli (script bench.sh).....	28
8.4 Correzioni al profilo NetworkManager.....	29
8.5 Risultati del benchmark.....	29
9. Confronto con la Letteratura Scientifica.....	30
Riferimenti Bibliografici.....	31

ELENCO DELLE FIGURE

Figura 1 — Schema architettura OSI 802.11: livelli PHY (PLCP + PMD) e MAC (DCF / EDCA) con raccordo LLC

Figura 2 — Tabella comparativa 802.11a/b/g: banda, modulazione, velocità massima e canali non sovrapposti

Figura 3 — Schema OFDM 802.11ac: aggregazione canali 20/40/80/160 MHz con sottoportanti e guard interval

Figura 4 — Linea del tempo IEEE 802.11 (1997–2024): velocità massima teorica, bande e denominazioni Wi-Fi 4/5/6/7

Figura 5 — Diagramma del 4-Way Handshake WPA2: quattro messaggi EAPOL con latenze tipiche per connessione

Figura 6 — Confronto frame FILS Discovery (89 byte) vs Beacon standard (335 byte) con tempistiche di trasmissione

Figura 7 — Gerarchia chiavi FILS: FILS-MK → FILS-SK → PMK con confronto rispetto alla gerarchia WPA2

Figura 8 — Confronto flusso roaming 802.11r (FT) vs FILS con indicazione dei round-trip eliminati

Figura 9 — Schema del banco di test: topologia con AP Fedora (hostapd), client Intel iwlwifi (CachyOS) e client Android

Figura 10 — Grafico a barre: tempi medi WPA2-PSK vs FILS-SHA256 con barre di errore (min/max)

Figura 11 — Grafico a linee: evoluzione dei tempi nei 10 run WPA2 vs 10 run FILS con evidenza della stabilizzazione

ELENCO DELLE TABELLE

Tabella 1 — Riepilogo standard IEEE 802.11 (1997–2024): anno, bande, velocità massima e innovazione chiave (§ 2.9)

Tabella 2 — Suite AKM FILS definite in IEEE 802.11-2020 (§ 4.4)

Tabella 3 — Architettura del banco di test: componenti, hardware, software e sistemi operativi (§ 6.1)

Tabella 4 — Risultati del benchmark: WPA2-PSK vs FILS-SHA256 (successi, media, min, max) (§ 8.5)

1. Introduzione

Questo lavoro di tesi nasce dall'esigenza di verificare se il protocollo IEEE 802.11ai, detto anche FILS (Fast Initial Link Setup), possa essere usato come soluzione adottabile in scenari con connessione senza cavo ad alta mobilità e alta densità di stazioni, dove i meccanismi di autenticazione tradizionali costituiscono una possibile limitazione. L'obiettivo non è puramente teorico poiché si è voluto verificare se FILS fosse implementabile su una generica workstation (come un notebook con hostapd) e su piattaforme open source più specializzate come OpenWrt, e misurarne i benefici in modo riproducibile.

La motivazione pratica per questa ricerca è emersa anche dall'esperienza maturata durante lo sviluppo di un sistema di distribuzione di servizi Wi-Fi in contesti privi di connettività Internet. In tale contesto — la configurazione di router GL-iNet con OpenWrt per un evento pubblico, in cui i partecipanti dovevano poter accedere a una Progressive Web App locale senza dipendere dalla navigazione nella rete internet — sono stati confrontati diversi profili di autenticazione wireless, tra cui WPA3-SAE, scelto per la sua robustezza e per le garanzie di forward secrecy anche in assenza di infrastruttura PKI. Tale esperienza ha evidenziato come, in scenari analoghi ma caratterizzati da alta mobilità delle stazioni riceventi (in genere sono smartphone), il tempo di autenticazione possa diventare un vincolo determinante. Valutare se FILS sia in grado di ridurlo a sufficienza da influenzare le scelte architetturali del sistema rappresenta una delle domande a cui questa tesi vuole proporre una risposta.

1.1 Contesto e motivazioni

La cifratura è un requisito fondamentale nelle reti wireless moderne, in particolare nei contesti critici — come le comunicazioni di emergenza, le reti veicolari e gli ambienti pubblici ad alta densità — dove i dati trasmessi possono includere informazioni sensibili quali cartelle cliniche o segnalazioni di sicurezza. Senza meccanismi di cifratura robusti, le reti risultano esposte a intercettazioni non autorizzate e alla diffusione di informazioni errate, con conseguenze potenzialmente gravi.

Lo standard attualmente più diffuso per l'autenticazione individuale sulle reti IEEE 802.11 è il protocollo WPA2-EAP (Wi-Fi Protected Access 2 — Extensible Authentication Protocol), noto anche come WPA2-Enterprise. Esso, tuttavia, presenta un limite significativo: la procedura di handshake richiede diversi secondi a causa della necessità di creare tunnel TLS e scambiare credenziali di autenticazione. Nella variante WPA2-PSK (Personal), il 4-Way Handshake standard introduce comunque latenze nell'ordine di 400–700 ms, incompatibili con applicazioni real-time.

Per ovviare a questo problema, il presente lavoro adotta e implementa il protocollo IEEE 802.11ai FILS (Fast Initial Link Setup), per ridurre drasticamente il tempo di setup del collegamento in modo da poter aumentare il volume dei dati trasmissibili in scenari con frequenti disconnessioni.

1.2 Obiettivi del progetto

- **Analizzare** accuratamente l'architettura teorica del protocollo FILS e confrontarla con gli standard collegati (WPA2-EAP, IEEE 802.11r).
 - **Implementare** un banco di test funzionante su hardware comune: Access Point su PC Fedora con hostapd compilato dai sorgenti, client su PC CachyOS con scheda Intel iwlwifi.
 - **Valutare** la fattibilità di FILS su piattaforme embedded tramite OpenWrt su Raspberry Pi 4.
 - **Raccogliere** dati quantitativi sui tempi di associazione FILS vs WPA2-PSK standard tramite uno script di benchmark affidabile e riproducibile.

1.3 Struttura del documento

Il Capitolo 2 traccia la storia degli standard IEEE 802.11 dalle origini fino a Wi-Fi 7, con focus sull'architettura MAC/PHY e l'evoluzione delle velocità.

Il Capitolo 3 descrive lo stato dell'arte dei protocolli di autenticazione.

Il Capitolo 4 illustra l'architettura teorica di FILS.

Il Capitolo 5 confronta FILS con IEEE 802.11r.

- | Il Capitolo 6 descrive l'implementazione dell'Access Point su Fedora.
- | Il Capitolo 7 riporta la valutazione su OpenWrt.
- | Il Capitolo 8 descrive dei benchmark e i relativi risultati.
- | Il Capitolo 9 presenta il confronto con la letteratura.

2. L'Evoluzione degli Standard IEEE 802.11

La famiglia di standard IEEE 802.11 costituisce oggi il fondamento tecnologico delle reti wireless locali in tutto il mondo. Nata alla fine degli anni Novanta come risposta alla crescente domanda di connettività senza fili in ambito aziendale e domestico, essa ha attraversato in poco meno di trent'anni una trasformazione radicale. Analizzare questa evoluzione è essenziale per capire le limitazioni degli standard precedenti e comprendere appieno le innovazioni introdotte da IEEE 802.11ai (FELS).

2.1 Architettura di riferimento: il modello MAC/PHY

Come ogni protocollo della famiglia IEEE 802, IEEE 802.11 riguarda i due livelli inferiori del modello ISO/OSI: il livello fisico (PHY) e il livello di collegamento (Data Link Layer). I livelli superiori — dal terzo (Network Layer) in su — rimangono invariati, consentendo un'implementazione trasparente tra reti wireless e cablate/Ethernet.

Il livello fisico (PHY)

Il livello fisico si occupa della trasmissione e ricezione dei segnali radio. Ogni generazione di 802.11 ha introdotto una nuova specifica PHY, caratterizzata da tecniche di modulazione, bande di frequenza e larghezze di canale diverse. Le principali tecniche utilizzate nel corso degli anni sono:

- **DSSS (Direct-Sequence Spread Spectrum):** utilizzata nelle prime versioni con la banda a 2,4 GHz. Quest'ultima è una banda suddivisa in 14 canali da 22 MHz ciascuno, di cui solo tre non sovrapposti (1, 6, 11). Questa tecnica usa una forma di trasmissione a spettro espanso in cui, attraverso dei codici di espansione, si distribuisce il segnale su una larghezza di banda maggiore di quella normalmente necessaria. Questo serve per aumentare la resistenza a rumore e interferenze. Di conseguenza una volta ricevuti i dati "spalmati", vanno ricostruiti con gli stessi codici di espansione.
- **OFDM (Orthogonal Frequency Division Multiplexing):** introdotta con 802.11a e poi adottata da tutte le generazioni successive. È una tecnica di trasmissione consistente in un tipo di modulazione a multi-portante, che utilizza cioè un numero elevato di sottoportanti tra loro ortogonali. Ciascuna di queste portanti è modulata attraverso una modulazione di tipo convenzionale (ad esempio una modulazione di

ampiezza in quadratura) con un basso symbol rate. Questo permette di comunicare anche in condizioni pessime del canale, ad esempio nei casi in cui si presenta un'attenuazione ad alta frequenza, come nei doppiini di rame, oppure interferenze a banda stretta. Mantenere un basso symbol rate permette di ridurre l'interferenza intersimbolica grazie ad intervalli di guardia di durata accettabile, oltre a garantire un'attenuazione più costante e perciò stimabile nonché correggibile.

- **MIMO (Multiple-Input Multiple-Output):** introdotta con 802.11n. L'utilizzo di più antenne in trasmissione e ricezione permette di sfruttare il multipath come risorsa anziché come disturbo, moltiplicando la capacità del canale (spatial multiplexing) o migliorando l'affidabilità (diversity).
- **MU-MIMO e OFDMA:** introdotti rispettivamente con 802.11ac (MU-MIMO in downlink) e 802.11ax (OFDMA bidirezionale). Consentono di servire più stazioni simultaneamente, aumentando l'efficienza spettrale in ambienti ad alta densità.

Il livello MAC

Il MAC gestisce l'accesso condiviso al canale radio. Poiché una stazione wireless non può trasmettere e ricevere simultaneamente sullo stesso canale, non è possibile rilevare le collisioni durante la trasmissione. IEEE 802.11 adotta quindi il protocollo CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Il meccanismo base è il **DCF (Distributed Coordination Function)**: prima di trasmettere, la stazione verifica la libertà di trasmissione sul canale per un intervallo minimo DIFS (*Distributed Inter Frame Space*). Se il canale è occupato, la stazione attende per una durata casuale (detto tempo di *backoff*), decrementandolo ogni volta che il canale è libero. La trasmissione avviene solo quando il contatore raggiunge zero. Ogni frame ricevuto correttamente viene confermato da un frame ACK inviato dopo un breve intervallo SIFS (*Short Inter Frame Space*, di durata inferiore al DIFS).

Accanto al DCF, lo standard definisce il PCF (Point Coordination Function) per il traffico a tempo garantito, e successivamente l'EDCA (Enhanced Distributed Channel Access, 802.11e) che introduce quattro code di accesso con priorità diverse — voce, video, best effort e background — fondamentali per il supporto QoS alle applicazioni multimediali.

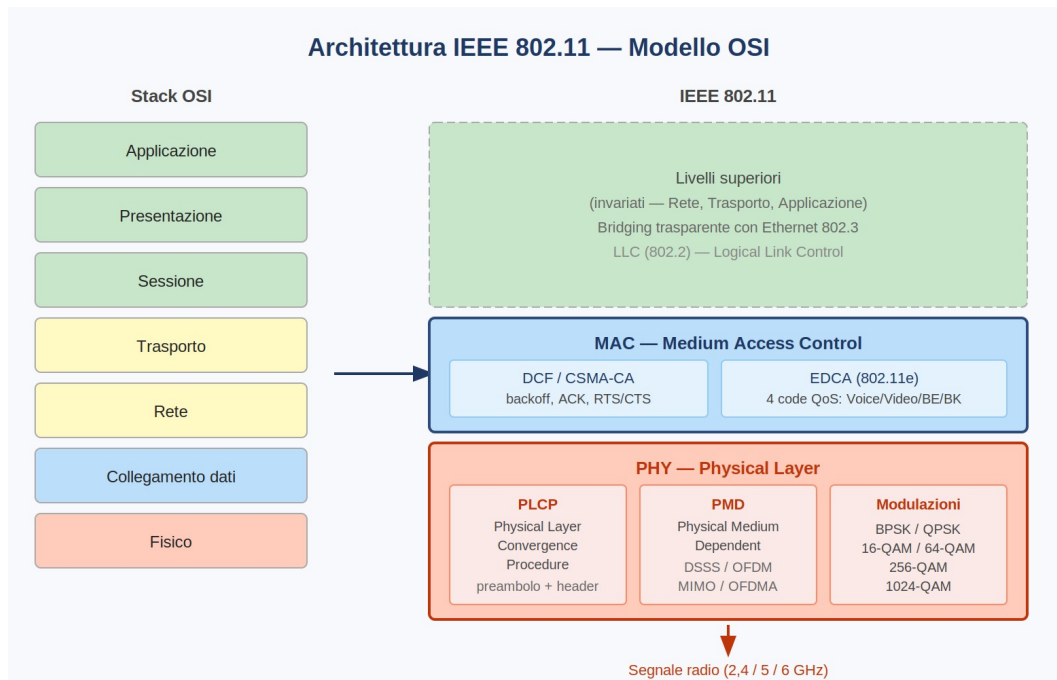


Figura 1: Schema architettura OSI 802.11: livelli PHY (PLCP + PMD) e MAC (DCF / EDCA)

2.2 Le origini: IEEE 802.11 legacy (1997) e 802.11b (1999)

L'IEEE 802.11 (modalità legacy) — o più correttamente IEEE 802.11-1997 o IEEE 802.11-1999 — si riferisce alla versione originale dello standard di rete wireless IEEE 802.11, rilasciata nel 1997 e chiarita nel 1999. La maggior parte dei protocolli descritti da questa prima versione sono oggi raramente utilizzati. Il testo di riferimento specificava due velocità di trasmissione di dati grezze di 1 e 2 megabit al secondo (Mbit/s) da trasmettere tramite segnali a infrarossi (IR), Frequency hopping o Direct-sequence spread spectrum (DSSS) nella banda di frequenza a 2,4 GHz. La tecnologia IR rimane parte dello standard, ma non ha implementazioni concrete. Lo standard originale definisce anche l'accesso multiplo con rilevamento della portante e prevenzione delle collisioni (attraverso i meccanismi CSMA/CA) al fine di migliorare l'affidabilità delle trasmissioni dati in condizioni ambientali diverse e avverse.

Nel luglio del 1999, l'IEEE ha introdotto la specifica 802.11b, che consente velocità teoriche fino a 11 Mbps, sebbene la larghezza di banda pratica sia più vicina ai 2 Mbps per TCP e ai 3 Mbps per UDP. Lo standard 802.11b utilizza la stessa frequenza di segnalazione radio non regolamentata (2,4 GHz) dello standard 802.11 originale. I produttori spesso preferiscono utilizzare queste frequenze per ridurre i costi di produzione. Questo comporta un

problema di interferenze risolvibile installando il dispositivo 802.11b a una distanza ragionevole dagli altri apparecchi. Lo standard 802.11b è anche informalmente noto come Wi-Fi 1.

2.3 La banda da 5 GHz e OFDM: IEEE 802.11a (1999)

Sviluppato parallelamente allo standard 802.11b, lo standard 802.11a offre velocità fino a 54 Mbps con segnali a 5 GHz. Sebbene, ai tempi, meno diffuso a causa dei costi più elevati, è stato utilizzato principalmente nelle reti aziendali, mentre l'802.11b era preferito per le reti domestiche. Inoltre, introduce l'utilizzo della banda dei 5 GHz, meno soggetta a interferenze rispetto ai 2,4 GHz, e adotta la modulazione OFDM (Orthogonal Frequency Division Multiplexing), una tecnica che suddivide il canale radio in molteplici sottoportanti ortogonali.

Grazie a OFDM e a canali da 20 MHz, 802.11a raggiunge una velocità fisica massima di 54 Mbps, un valore nettamente superiore rispetto agli 11 Mbps di 802.11b. Tuttavia, l'utilizzo della banda a 5 GHz comporta una portata inferiore: le frequenze più elevate subiscono un'attenuazione maggiore e penetrano con più difficoltà muri e ostacoli, rendendo lo standard meno adatto agli ambienti domestici dell'epoca. Poiché 802.11a e 802.11b operano su bande di frequenza differenti e utilizzano schemi di modulazione incompatibili (OFDM per 802.11a, DSSS/CCK per 802.11b), i due standard non sono interoperabili. In classificazioni retroattive introdotte dalla Wi-Fi Alliance, 802.11a è talvolta indicato come Wi-Fi 2.

2.4 La sintesi: IEEE 802.11g (2003)

Introdotta nel 2003, lo standard 802.11g combina le caratteristiche degli standard 802.11a e 802.11b, supportando velocità fino a 54 Mbps e utilizzando la frequenza a 2,4 GHz per una maggiore portata, mantenendo comunque la retrocompatibilità con lo standard 802.11b. Lo standard 802.11g è anche informalmente noto come Wi-Fi 3.

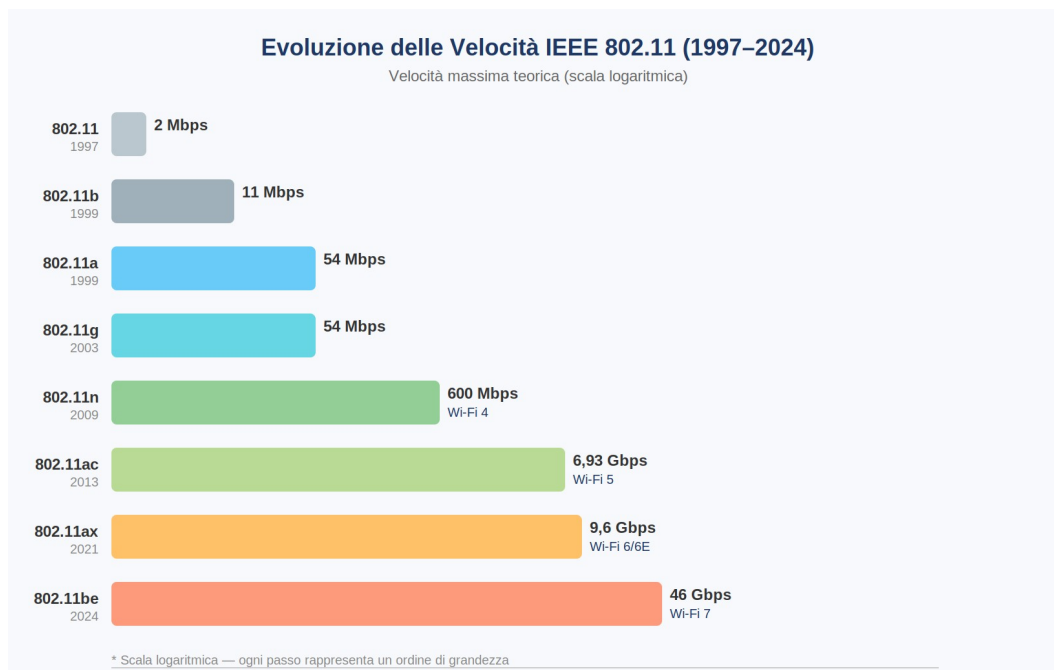


Figura 2: Tabella comparativa 802.11a/b/g: banda, modulazione, velocità massima e canali non sovrapposti

2.5 La rivoluzione MIMO: IEEE 802.11n (2009) — Wi-Fi 4

Lo standard 802.11n (noto come Wireless N) è stato progettato per migliorare le prestazioni dello standard 802.11g. Ratificato nel 2009, è il primo standard Wi-Fi a supportare entrambe le bande di frequenza a 2,4 GHz e 5 GHz ed è in grado di utilizzarle entrambe contemporaneamente operando in modalità dual-band *selectable*. L'802.11n è la prima generazione di Wi-Fi a supportare il trasferimento dati MIMO (multiple in, multiple out). Il MIMO consente a un router di utilizzare fino a quattro antenne contemporaneamente in ricezione e trasmissione e permette di distribuire più flussi spaziali su un singolo canale radio, aumentando sia la portata del segnale che la sua velocità di trasmissione complessiva. In condizioni ideali, un router o un access point 802.11n può trasmettere dati fino a 600 Mbps, limite maggiore dei 54 Mbps dell'802.11g. Tuttavia, poiché la banda a 5 GHz è più suscettibile alle interferenze provenienti da muri e altri oggetti fisici, le velocità di utilizzo reali si attestano spesso tra i 100 e i 200 Mbps.

2.6 Il gigabit wireless: IEEE 802.11ac (2013) — Wi-Fi 5

IEEE 802.11ac, detto anche Wi-Fi 5, aumenta ancora una volta la velocità di trasmissione grazie a diverse migliorie:

Canali fino a 80 MHz: lo standard 802.11n utilizzava fino a quattro flussi spaziali e canali con larghezza di banda di 40 MHz per realizzare la tecnologia MIMO (Multiple Input, Multiple Output). Lo standard 802.11ac, invece, utilizza otto flussi spaziali e canali con larghezza di banda fino a 80 MHz. Per supportare il MIMO, i router sono sempre più spesso progettati con antenne multiple.

Modulazione 256-QAM (8 bit/simbolo anziché 6 di 64-QAM): lo standard 802.11ac utilizza la modulazione QAM a 256 livelli, rispetto alla QAM a 64 livelli dello standard 802.11n. Ciò significa che lo standard 802.11ac utilizza una costellazione di 256 punti, codificando 8 bit per simbolo invece dei 6 bit di 64-QAM. In teoria, l'efficienza spettrale dello standard 802.11ac aumenta di circa il 33% rispetto a quella dello standard 802.11n.

Beamforming: questa tecnologia invia le trasmissioni in modo direzionale anziché a 360 gradi, come avveniva nella maggior parte delle tecnologie wireless prima dell'avvento dello standard 802.11ac. Il beamforming si ottiene utilizzando più antenne sul router: l'AP applica pesi di fase e ampiezza ai segnali delle antenne per concentrare l'energia verso il client.

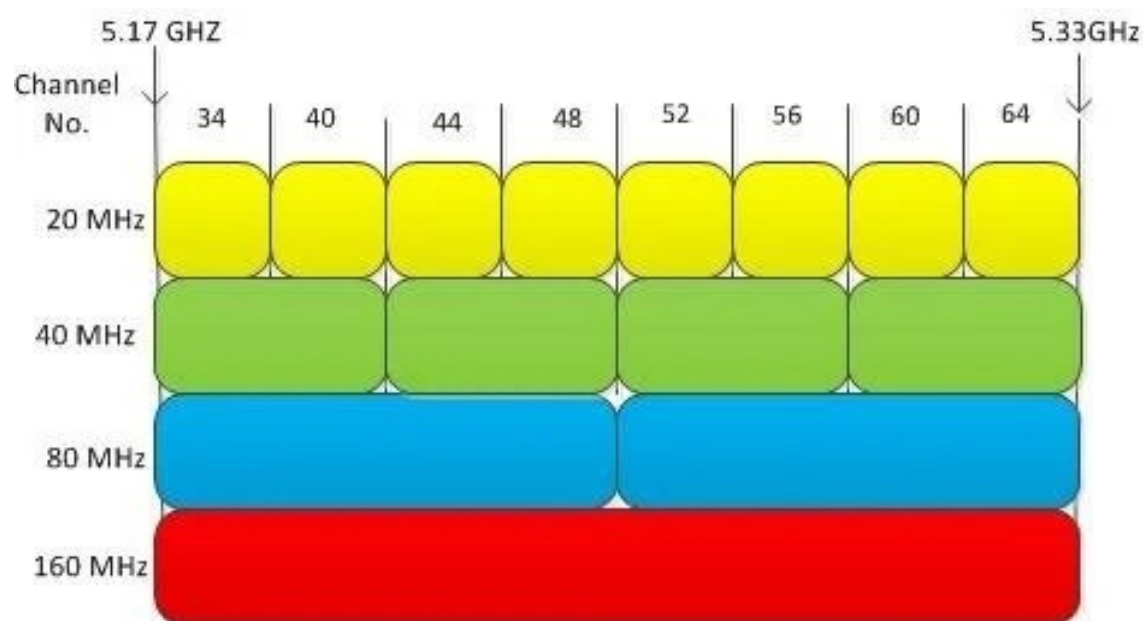


Figura 3: Schema OFDM 802.11ac: aggregazione canali 20/40/80/160 MHz

2.7 L'era della densità: IEEE 802.11ax (2021) — Wi-Fi 6 e 6E

IEEE 802.11ax, denominato Wi-Fi 6 (e Wi-Fi 6E per la variante a 6 GHz), segna un cambiamento di paradigma: il focus non è più solo sulla velocità di picco, ma sull'efficienza in ambienti ad altissima densità.

Lo standard 802.11ax introduce anche l'OFDMA, un nuovo meccanismo di accesso al canale simile ma distinto dalle reti radio cellulari/LTE, in quanto mantiene la robustezza dello spettro del Wi-Fi. In primo luogo, l'OFDMA garantisce una trasmissione con minima contesa a più client sia in downlink (DL) che in uplink (UL) all'interno di una singola opportunità di trasmissione (TXOP). In secondo luogo, l'aggiunta del HE-EDCA (High Efficiency EDCA) consente all'access point di influenzare le priorità di accesso al canale relative dei client, anche tra 11ax e 11ac. Entrambi gli schemi non solo sono più efficienti e meno soggetti a perdita di pacchetti e jitter dovuti alla contesa, ma, poiché consentono all'access point di avere un controllo preciso sia sulle trasmissioni in uplink che in downlink, permettono anche un maggiore determinismo. Una novità importante riguarda il MU-MIMO, che consente all'access point di gestire più flussi spaziali verso più client contemporaneamente, offrendo prestazioni migliorate.

Lo standard introduce inoltre la modulazione 1024-QAM, che aumenta l'efficienza spettrale del 25% rispetto a 256-QAM, sebbene sia utilizzabile solo in condizioni radio ottimali. Con Wi-Fi 6E, l'apertura della banda 6 GHz permette l'uso di canali più ampi e meno congestionati, migliorando ulteriormente throughput e latenza.

2.8 Verso il futuro: IEEE 802.11be (2024) — Wi-Fi 7

IEEE 802.11be, commercialmente denominato Wi-Fi 7, è stato ratificato nel 2024. Le innovazioni principali sono: la tecnologia Multi-Link Operation (MLO), che consente ai dispositivi di utilizzare più link radio simultaneamente, anche su bande diverse (2,4 GHz, 5 GHz e 6 GHz) o su più canali all'interno della stessa banda. Ciò non solo offre prestazioni di throughput più elevate, ma contribuisce anche a ridurre la latenza e permette ai dati di fluire senza ostacoli dovuti al traffico di rete o alle interferenze; canali da 320 MHz sulla banda 6 GHz; aumenta la modulazione QAM da 1024 a 4096 (12 bit/simbolo); Un altro miglioramento chiave riguarda il MU-MIMO, che in 802.11be supporta fino a 16 flussi spaziali, raddoppiando il limite di 802.11ax. Questo consente a un access point di servire un numero maggiore di client in parallelo. Lo standard introduce anche HARQ (Hybrid Automatic Repeat reQuest), una tecnica mutuata dalle reti cellulari che migliora l'affidabilità riducendo la necessità di ritrasmettere interi frame, insieme a meccanismi come il Restricted Target

Wake Time (rTWT) e il preamble puncturing avanzato. L'insieme di queste migliorie porta la velocità teorica massima sui 46 Gbps.

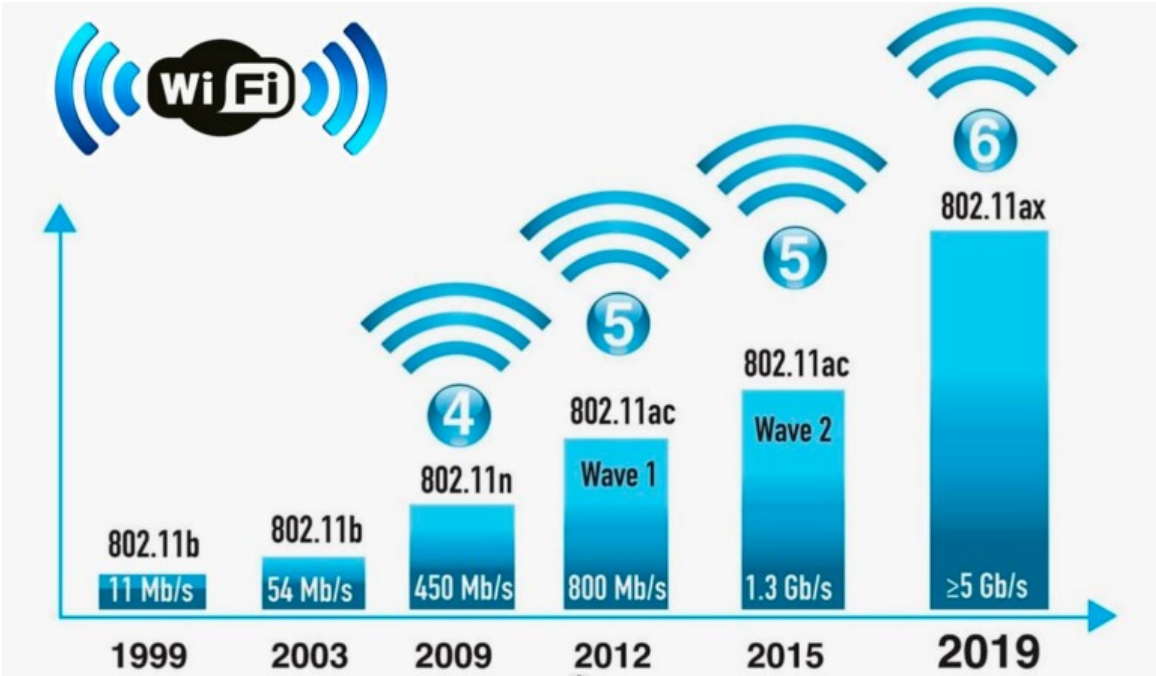


Figura 4: Linea del tempo IEEE 802.11 (1997–2024): velocità massima teorica, bande e denominazioni Wi-Fi 4/5/6/7

2.9 Riepilogo e motivazione per FILS

Standard	Anno	Bande (GHz)	Vel. max	Innovazione chiave
802.11 legacy	1997	2,4	2 Mbps	DSSS/FHSS — fundamenta MAC/PHY
802.11b	1999	2,4	11 Mbps	CCK, prima adozione di massa
802.11a	1999	5	54 Mbps	OFDM, banda 5 GHz
802.11g	2003	2,4	54 Mbps	OFDM su 2,4 GHz, retrocompat. b
802.11n / Wi-Fi 4	2009	2,4 / 5	600 Mbps	MIMO, canali 40 MHz, A-MPDU
802.11ac / Wi-Fi 5	2013	5	6,93 Gbps	MU-MIMO DL, 160 MHz, 256-QAM
802.11ax / Wi-Fi 6/6E	2021	2,4/5/6	9,6 Gbps	OFDMA, TWT, 1024-QAM
802.11be / Wi-Fi 7	2024	2,4/5/6	46 Gbps	MLO, 320 MHz, 4096-QAM

L'analisi di questa evoluzione evidenzia un fatto paradossale: mentre le velocità di trasmissione sono aumentate di oltre quattro ordini di grandezza in venticinque anni, il meccanismo di autenticazione e associazione — la procedura che ogni dispositivo deve completare prima di poter trasmettere dati — è rimasto sostanzialmente invariato. In un'era in cui un singolo frame 802.11ax può trasportare decine di megabit in pochi millisecondi, un handshake che richiede centinaia di millisecondi o addirittura secondi rappresenta un collo di bottiglia sempre più anacronistico. È proprio per colmare questo divario che è stato sviluppato IEEE 802.11ai (FILS), descritto nel Capitolo 4.

3. Protocolli di Autenticazione IEEE 802.11: Stato dell'Arte

I principali protocolli di autenticazione individuale per le reti IEEE 802.11 sono definiti negli standard IEEE 802.11i e IEEE 802.1X, collettivamente noti come WPA2-EAP. Questi protocolli consentono ad access point e stazioni di identificarsi reciprocamente tramite certificati digitali o coppie di credenziali. Il framework Extensible Authentication Protocol (EAP) offre una varietà di metodi di autenticazione.

3.1 Metodi EAP principali

EAP-TLS

Definito nella RFC 5216, è ampiamente considerato lo standard di riferimento per l'autenticazione Wi-Fi. Utilizza un'autenticazione reciproca basata su certificati: sia il dispositivo client che il server RADIUS presentano certificati digitali per dimostrare la propria identità. Non essendo coinvolte password, EAP-TLS è completamente immune a phishing, attacchi di forza bruta, credential stuffing e attacchi man-in-the-middle.

EAP-PEAP

PEAP (Protected Extensible Authentication Protocol), definito nella RFC 7170, è il metodo EAP più diffuso negli ambienti aziendali. Crea un tunnel TLS sicuro utilizzando un certificato lato server; quindi, autentica il client all'interno di tale tunnel tramite nome utente e password, più comunemente tramite MS-CHAPv2. La popolarità di PEAP deriva dal suo equilibrio tra un buon livello di sicurezza e una semplice implementazione. Poiché gli utenti si autenticano con le proprie credenziali Active Directory o LDAP esistenti, non è necessaria la gestione di un'infrastruttura di certificati lato client. Richiede comunque uno scambio EAP completo durante la configurazione del collegamento sicuro, comportando latenze non trascurabili — tipicamente tra 1 e 5 secondi.

3.2 Limiti del WPA2-EAP in scenari ad alta mobilità

Studi precedenti hanno evidenziato che i ritardi di autenticazione WPA2-EAP aumentano proporzionalmente alla densità dei veicoli nella rete. In scenari ad alta densità, i ritardi di assegnazione degli indirizzi IP e di autenticazione causano una riduzione significativa della velocità di trasmissione inter-veicolare. Diversi ricercatori hanno proposto approcci basati

su pre-autenticazione o caching delle chiavi, ma nessuno ha affrontato pienamente lo scenario veicolare né fornito un'implementazione open source misurabile su hardware commerciale.

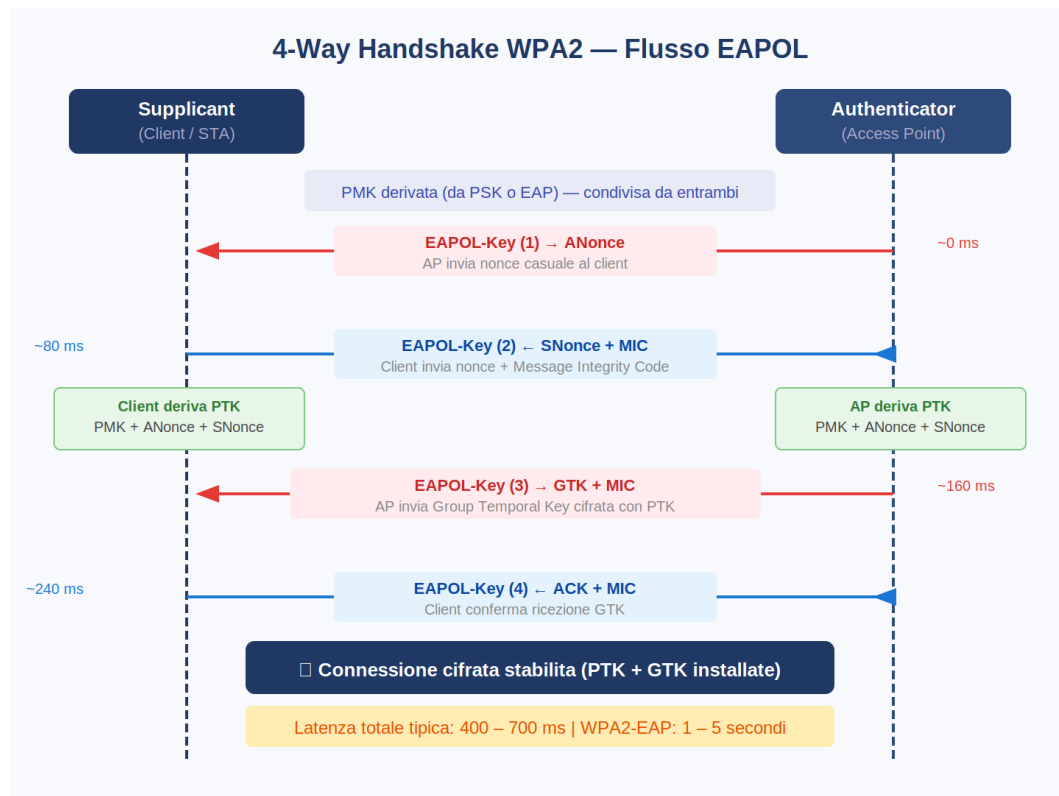


Figura 5: Diagramma del 4-Way Handshake WPA2: quattro messaggi EAPOL con latenze tipiche per connessione

3.3 WPA3: evoluzione della sicurezza wireless

Wi-Fi Protected Access 3 (WPA3) è stato introdotto dalla Wi-Fi Alliance nel 2018 come successore di WPA2, con l'obiettivo di correggere le vulnerabilità strutturali emerse negli anni e di adeguare la sicurezza wireless alle esigenze contemporanee. Lo standard si divide in WPA3-Personal e WPA3-Enterprise.

WPA3-Personal sostituisce il vecchio Pre-Shared Key (PSK) usato da WPA2 con il SAE (Simultaneous Authentication of Equals): appartiene a una famiglia di protocolli noti come Password-Authenticated Key Exchanges (PAKE), che permettono a due dispositivi di dimostrare di conoscere entrambi la stessa password senza mai inviarla né scambiarsela in chiaro. Per raggiungere questo obiettivo, WPA3 utilizza l'handshake Dragonfly, un proces-

so in due fasi in cui il client e l'access point si scambiano valori crittografici speciali (messaggi di commit e confirm). Questi valori fungono da prova della correttezza della password, senza però rivelarla. Il risultato è una password condivisa, univoca per ogni connessione client-AP, che diventa poi la base per la Pairwise Master Key (PMK). Questa architettura garantisce anche la forward secrecy, in modo che, anche se la password Wi-Fi viene rubata in un secondo momento, il traffico precedentemente intercettato rimanga protetto.

WPA3-Enterprise (modalità standard): supporta EAP-TLS, PEAP e EAP-TTLS. Richiede i Protected Management Frame (PMF) e suite crittografiche più robuste rispetto a WPA2, ma non impone un metodo EAP specifico. WPA3-Enterprise a 192 bit (modalità ad alta sicurezza): richiede EAP-TLS con autenticazione basata su certificati. Utilizza algoritmi crittografici della Suite B (suite CNSA) tra cui crittografia AES-256-GCM, hashing SHA-384 e certificati ECDSA-384 o RSA-3072+. Questa modalità è progettata per implementazioni nei settori governativo, della difesa e finanziario, dove è richiesta la conformità allo standard NIST SP 800-120.

Nel contesto di un “lavoro sul campo”, WPA3-SAE è stato valutato come possibile parte di una configurazione di alcuni router GL-iNet Flint 2 con OpenWrt, utilizzati durante un evento pubblico per distribuire una Progressive Web App locale in assenza di connettività Internet, proprio per sfruttare il forward secrecy. Tuttavia, in quello scenario la mobilità delle stazioni era limitata e i tempi di associazione non erano un vincolo critico. È proprio questa differenza rispetto agli scenari veicolari e ad alta mobilità che motiva lo studio di FILS come complemento o alternativa ai meccanismi di autenticazione standard, incluso WPA3.

4. FILS — Fast Initial Link Setup (IEEE 802.11ai)

FILS è un insieme di meccanismi standardizzati in IEEE 802.11ai (2016) e successivamente incorporati nello standard principale IEEE 802.11-2020. L'obiettivo è ridurre il tempo necessario per la configurazione iniziale del collegamento agendo su tutte e tre le fasi: discovery, autenticazione/associazione e configurazione dell'indirizzo IP. FILS consente di completare l'intero setup in circa 100 ms, rispetto ai diversi secondi richiesti da WPA2-EAP.

4.1 FILS Discovery: ottimizzazione della scansione dei canali

Tradizionalmente, i client IEEE 802.11 effettuano una scansione attiva inviando frame di Probe Request a tutti gli access point disponibili. Poiché tali frame non hanno un tempo di scadenza, ogni AP deve rispondere individualmente, generando traffico aggiuntivo sul canale e riducendo il throughput del data link.

FILS introduce due meccanismi per ottimizzare la fase di discovery:

- **Frame FILS Discovery:** gli AP trasmettono frame di scoperta ogni 20 ms (circa 20 TU), oltre ai normali beacon inviati ogni 100 ms. Questi frame sono più leggeri dei beacon standard (circa 89 byte vs. 335 byte).
- **Probe Deferral e Suppression:** Prima che la stazione client invii una richiesta di probing, deve rimanere in ascolto dei beacon broadcast e delle risposte di probing per un periodo di tempo detto Probe Delay time. Quando la stazione client invia una richiesta di probing, deve elencare gli AP di cui è già a conoscenza. Questo permetterà agli AP di sopprimere le proprie risposte.

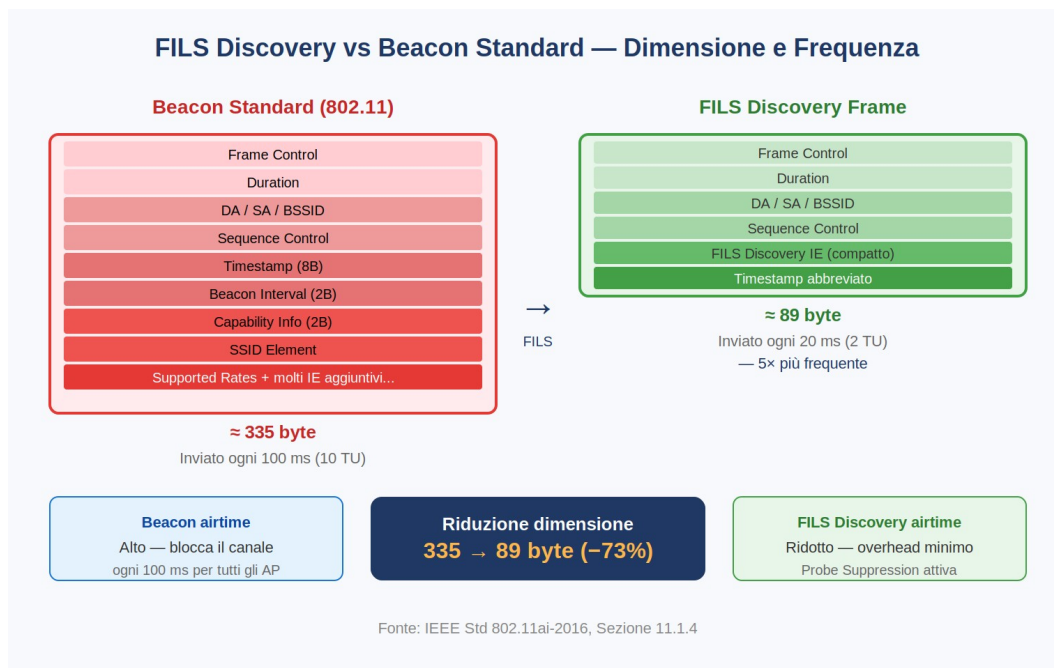


Figura 6: Confronto frame FILS Discovery (89 byte) vs Beacon standard (335 byte) con tempistiche di trasmissione

4.2 Assegnazione dell'indirizzo IP durante l'associazione con FILS

Nel processo Wi-Fi tradizionale, l'assegnazione dell'indirizzo IP avviene **solo dopo l'associazione**, tramite un normale scambio DHCP. Lo standard **IEEE 802.11ai (FILS)** anticipa questa fase integrando i messaggi DHCP direttamente nei frame di autenticazione, riducendo così il numero di round-trip necessari per completare il collegamento.

Questo è possibile grazie al **FILS HLP (Higher Layer Protocol) Container Element**, un elemento informativo che permette di **incapsulare pacchetti di livello superiore (EAP, DHCP, RSN, ecc.) all'interno dei frame 802.11**. In questo modo, la stazione può ricevere l'indirizzo IP già durante la fase di autenticazione, senza attendere la conclusione dell'associazione.

L'uso dell'HLP Container è particolarmente vantaggioso quando viene impiegato **ERP (EAP Re-authentication Protocol)**. ERP consente una riautenticazione rapida basata su chiavi derivate (vedere paragrafo successivo), evitando un full EAP. In combinazione con FILS, l'intero processo può essere ridotto a **un singolo messaggio di richiesta e un singolo messaggio di risposta**, entrambi contenenti i pacchetti EAP e DHCP necessari. Questo approccio riduce drasticamente i tempi dell'intero processo.

4.3 Caching delle informazioni di autenticazione

Durante la prima autenticazione tra una stazione e un access point, FILS consente di derivare e memorizzare una serie di chiavi (ad esempio rRK e rIK) che possono essere riutilizzate nelle connessioni successive. Questo meccanismo permette di evitare un nuovo scambio EAP completo, riducendo in modo significativo il numero di frame necessari per ristabilire un collegamento sicuro.

A partire dalla seconda connessione, la stazione può utilizzare le chiavi memorizzate per eseguire una **FILS Reauthentication**, che richiede soltanto uno scambio di richiesta e risposta. Oppure quando si tenta la connessione a un AP diverso ma con lo stesso ESS, si può utilizzare la modalità **FILS Opportunistic**, con uso di una PMK precedentemente ottenuta, completando la configurazione con un numero di scambi di frame nettamente inferiore.

Questo meccanismo è il fondamento operativo del comportamento misurato nei test del Capitolo 8: FILS opportunistic si attiva solo se esiste già una PMKSA (Pairwise Master Key Security Association) valida derivata da una prima autenticazione completata con successo.

4.4 Suite AKM e certificazione Wi-Fi

IEEE 802.11-2020 definisce quattro suite AKM (Authentication and Key Management) per FILS:

Suite AKM	Descrizione
00-0F-AC [14]	FILS con SHA-256 e AES-SIV-256
00-0F-AC [15]	FILS con SHA-384 e AES-SIV-512
00-0F-AC [16]	FT over FILS con SHA-256 e AES-SIV-256
00-0F-AC [17]	FT over FILS con SHA-384 e AES-SIV-512

FILS è incluso nella certificazione Wi-Fi Alliance denominata 'Wi-Fi Optimized Connectivity' (OCE — Optimized Connectivity Experience). Il supporto viene dichiarato dai client nel campo 'Extended Capabilities' (ottetto 10) dei frame Probe Request.

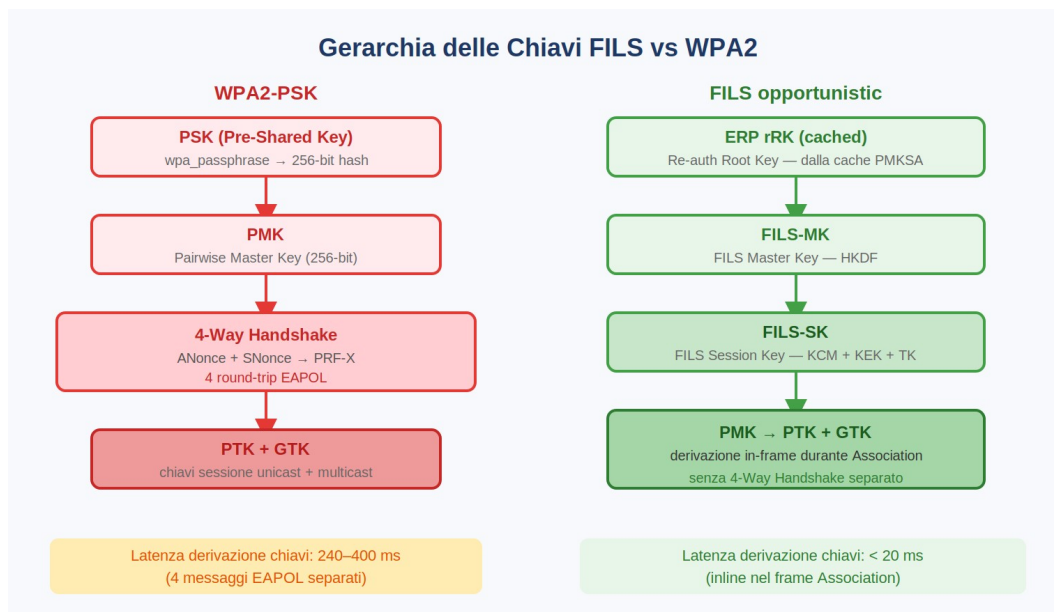


Figura 7: Gerarchia chiavi FILS: FILS-MK → FILS-SK → PMK con confronto rispetto alla gerarchia WPA2

5. Confronto tra FILS e IEEE 802.11r (Fast Transition)

Anche lo standard IEEE 802.11r (Fast BSS Transition, FT) serve per accelerare il roaming tra access point. A differenza di FILS, 802.11r si basa su chiavi pre-condivise PMK-R1 distribuite tra gli AP dello stesso dominio di mobilità. Il limite principale di 802.11r è la dipendenza dalla disponibilità di una chiave PMK-R1 valida: in assenza di questa chiave — ad esempio durante lo spostamento tra domini di mobilità distinti — il client deve eseguire un'autenticazione completa. Inoltre, 802.11r richiede che tutti gli AP del dominio condividano la stessa PMK-R0.

5.1 Il vantaggio di FILS rispetto a 802.11r

Anche in assenza di una PMK-R1 memorizzata, FILS esegue un'autenticazione sicura tramite le chiavi ERP. Il processo si svolge in quattro fasi:

- **Fase 1 — Invio** richiesta con un ID sessione FILS all'AP target.
- **Fase 2 — Risposta di autenticazione FILS:** l'AP valida il client tramite chiavi ERP da cui si calcola una nuova FILS Master Key (FILS-MK) e invia un KCM (messaggio di conferma).

- **Fase 3 — Derivazione delle chiavi e associazione:** dopo che la PMK viene calcolata dinamicamente, il client invia una richiesta di riassociazione con la FILS-SK.
- **Fase 4 — Connessione immediata:** il client viene connesso con le chiavi di sessione FILS appena derivate.

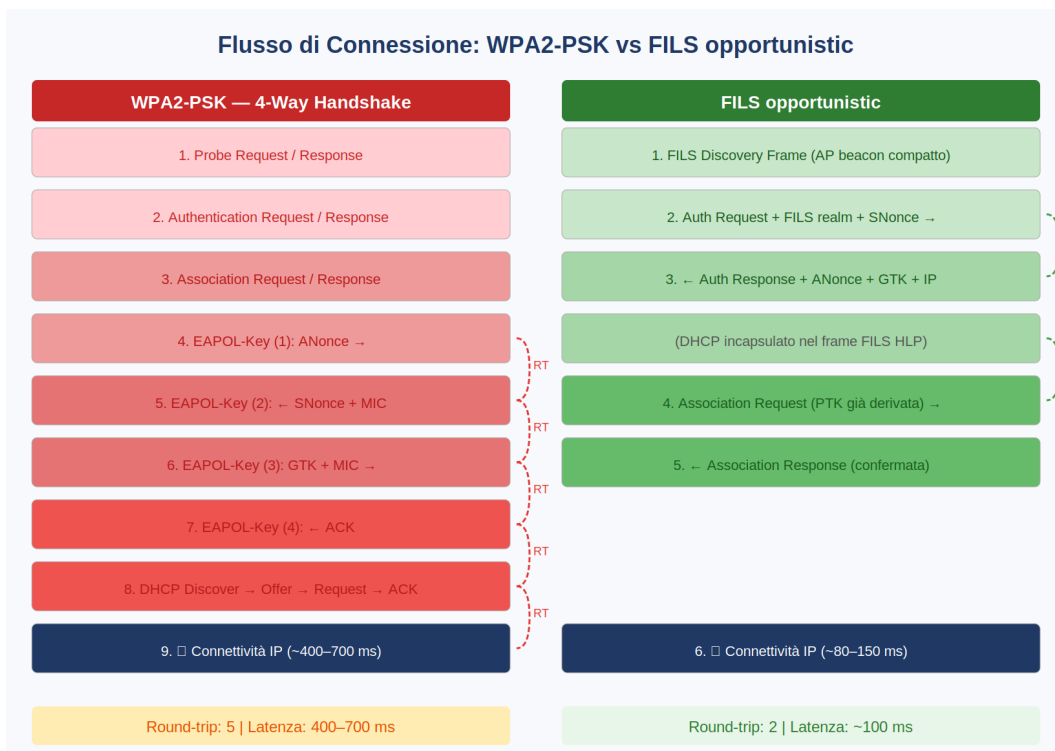


Figura 8: Confronto flusso roaming 802.11r (FT) vs FILS con indicazione dei round-trip eliminati

6. Fase 1 — Implementazione dell'Access Point FILS su Fedora

6.1 Architettura del banco di test

Componente	Hardware	Software / Ruolo	Sistema Operativo
Access Point (AP)	PC — wlp1s0 (Realtek RTL8852BE)	hostapd 2.11 da sorgente, dnsmasq (DHCP), firewallld (NAT)	Fedora 43, kernel 6.18
Client benchmark	PC — Intel iwlwifi (AX series)	NetworkManager 1.54.3, wpa_supplicant FILS	CachyOS, kernel 6.18
Client secondario	Smartphone Android (Redmi Note 12 Pro)	Validazione connettività consumer	Android
Backhaul	Interfaccia Ethernet enp3s0	Subnet 192.168.8.x → Internet	—

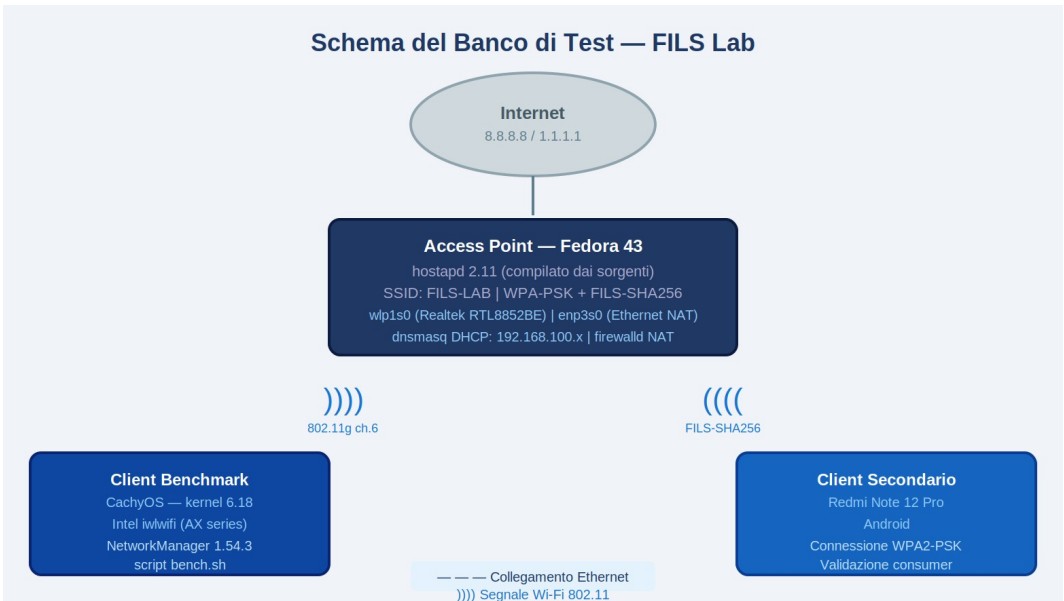


Figura 9: Schema del banco di test: topologia con AP Fedora (hostapd), client Intel iwlwifi (CachyOS) e client Android

6.2 Compilazione di hostapd con supporto FILS

Il pacchetto hostapd precompilato in Fedora 43 non include il supporto FILS. È stato necessario compilare manualmente dal repository ufficiale.

```
git clone git://w1.fi/hostap.git && cd hostap/hostapd
cp defconfig .config
echo "CONFIG_FILS=y" >> .config && echo "CONFIG_FILS_SK_PFS=y"
>> .config
echo "CONFIG_EAP=y" >> .config && echo "CONFIG_ERP=y" >> .config
echo "CONFIG_FULL_DYNAMIC_VLAN=y" >> .config
make clean && make -j$(nproc)
```

Durante la prima build sono emersi errori di linking (undefined reference to 'wpa_select_vlan_wpa_group'). Causa: il codice ERP usato da FILS dipende dal supporto EAP completo anche per configurazioni PSK senza RADIUS. Le flag mancanti erano CONFIG_EAP=y, CONFIG_ERP=y e CONFIG_FULL_DYNAMIC_VLAN=y. Soluzione: aggiunta di tutte le flag necessarie e make clean prima di ricompilare.

La compilazione del wpa_supplicant custom per il client ha incontrato un problema separato: fatal error: openssl/engine.h: No such file or directory. Soluzione: disabilitare esplicitamente CONFIG_OPENSSL_ENGINE nel .config di wpa_supplicant.

6.3 Configurazione dell'Access Point

Il file di configurazione hostapd-fils.conf per l'SSID FILS-LAB:

```
interface=wlp1s0 | driver=nl80211 | ssid=FILS-LAB | hw_mode=g |
channel=6
wpa=2 | wpa_key_mgmt=WPA-PSK FILS-SHA256 | wpa_psk=<hash_64_hex>
fils_realm=example.com | fils_cache_id=1234 | erp_domain=example.-
com | ieee80211w=2
```

Note critiche: il campo wpa_psk richiede un hash esadecimale a 64 caratteri (wpa_passphrase FILS-LAB MyPassword). ieee80211w=2 (PMF obbligatorio) è richiesto da FILS. La combinazione WPA-PSK + FILS-SHA256 in wpa_key_mgmt permette al client Android di connettersi con sola password. Il fils_cache_id deve corrispondere esattamente al valore memorizzato dal client: un mismatch invalida la cache e forza il fallback al 4-Way Handshake senza alcun avviso nei log.

6.4 Infrastruttura DHCP e NAT

La configurazione dnsmasq (port=0 per solo DHCP, DNS pubblici distribuiti direttamente) è necessaria perché systemd-resolved ascolta solo su 127.0.0.53 e non è raggiungibile dai client di rete.

Il routing NAT tramite firewalld ha richiesto: wlp1s0 (AP) → zona internal con --add-forward; enp3s0 (Ethernet) → zona public con masquerade; tun0 (VPN/SSH) → zona trusted. Diagnosi del blocco FORWARD: il log del kernel mostrava filter_FWD_internal_REJECT. Soluzione: ip_forward=1 e net.ipv4.conf.wlp1s0.rp_filter=0.

6.5 Conflitti con NetworkManager e KDE

Durante i test è emerso un conflitto critico: NetworkManager e plasmashell tentavano di scansionare reti wireless mentre l'interfaccia era in modalità AP, generando interferenze con hostapd. Soluzione: wlp1s0 impostata come unmanaged in NetworkManager, lasciandola in uso esclusivo ad hostapd.

6.6 Risultati della Fase 1

- Connessione Android funzionante con sola password (WPA2-PSK + FILS-SHA256 coesistenti).
- Assegnazione IP via DHCP corretta nella subnet 192.168.100.x.
- Navigazione Internet completa attraverso NAT.
- Log dettagliati disponibili per analisi dei tempi FILS.

Limitazione rilevata: il setup su Fedora richiede configurazione manuale complessa e risulta fragile rispetto a riavvii del sistema. Questo ha motivato la valutazione della piattaforma OpenWrt descritta nel Capitolo 7.

7. Fase 2 — Valutazione di OpenWrt su Raspberry Pi 4

7.1 Obiettivo e motivazioni

L'idea era verificare se OpenWrt su Raspberry Pi 4 potesse offrire una piattaforma più pulita e riproducibile per il testbed FILS, con configurazione persistente tramite UCI e dnsmasq/firewall già integrati.

7.2 Problemi di connettività riscontrati

La configurazione di default di OpenWrt presentava una subnet incompatibile con la rete domestica (FritzBox 192.168.178.0/24): OpenWrt LAN era impostata su 192.168.1.0/24, con eth0 incluso nel bridge br-lan, rendendo impossibile il suo uso come WAN. Un tentativo con adattatore USB-Ethernet Realtek (kmod-usb-net-r8152) è fallito per assenza del modulo nell'immagine — un classico problema di bootstrap. Soluzione: modifica dell'IP LAN a 192.168.178.200 e integrazione diretta nella rete FritzBox.

7.3 Limitazione critica: assenza di FILS in wpad-basic

OpenWrt utilizza di default wpad-basic, versione ridotta di hostapd compilata per minimizzare l'ingombro su dispositivi con storage limitato. wpad-basic esclude il supporto a EAP, RADIUS, PMF e FILS.

7.4 Conclusioni sulla piattaforma embedded

Il Raspberry Pi 4 non è risultato adeguato come piattaforma per test avanzati su FILS nella configurazione attuale di OpenWrt. La ricerca su IEEE 802.11ai richiede un sistema x86 con driver Intel (AX200/AX210) e hostapd compilato dai sorgenti. L'esperienza ha comunque fornito indicazioni utili: wpad-openssl o wpad-wolfssl sono le versioni necessarie, e la loro installazione richiede la rimozione preventiva di wpad-basic tramite opkg o apk.

8. Fase 3 — Benchmark FILS: Setup, Metodologia e Risultati

8.1 Setup del client di benchmark

La macchina client è un PC con CachyOS (kernel 6.18) e scheda Wi-Fi Intel (driver iwlwifi). L'AP rimane il PC Fedora configurato nella Fase 1. La metrica di riferimento è il tempo totale di associazione: l'intervallo tra la disconnessione e il ripristino della connettività IP.

8.2 Scoperta chiave: il ruolo della cache FILS

Durante i primi test è emerso un comportamento fondamentale: FILS opportunistic funziona esclusivamente dopo che il client ha memorizzato i parametri crittografici derivati da una prima autenticazione WPA2-PSK standard. Questa cache include il FILS realm, i parametri della PSK, le informazioni sull'AP (BSSID, canale) e la PMKSA.

Osservazione pratica: la connessione FILS funzionava perfettamente quando era NetworkManager/KDE a gestirla, ma falliva con script bash che usavano wpa_supplicant avviato manualmente — il quale non ha accesso alla cache. Questa osservazione ha orientato la strategia di benchmark verso il riuso dei profili NetworkManager esistenti.

8.3 Evoluzione degli script di benchmark

Il percorso verso uno script affidabile ha attraversato quattro iterazioni:

Tentativo 1 — wpa_supplicant manuale (bash)

Race condition sul socket ctrl_interface, conflitti con NetworkManager, driver Intel che rifiutava richieste FILS dopo kill/restart aggressivo. Risultato: timeout sistematici.

Tentativo 2 — Python con D-Bus (pydbus)

Segnali D-Bus inaffidabili, proprietà stale per caching di pydbus, profili NM duplicati con configurazione conflittuale. Risultato: parzialmente funzionante ma fragile.

Tentativo 3 — Python con nmcli (subprocess)

Più stabile del D-Bus diretto, ma verboso e con parsing complesso.

Soluzione finale — bash + nmcli (script bench.sh)

Il punto di svolta è arrivato dalla scoperta della sequenza nmcli corretta: ¹

```
nmcli connection modify <uuid> 802-11-wireless-security.fils 1
nmcli device wifi rescan && nmcli device disconnect wlan0
sleep 1 && timeout 45 nmcli connection up <uuid>
```

Questa sequenza funziona perché: (1) modifica il parametro FILS preservando la cache; (2) aggiorna i beacon visibili dal driver; (3) pulisce lo stato del driver in modo pulito; (4) riconnette usando il profilo con cache FILS già popolata. Lo script finale bench.sh crea due profili NM separati (FILS-Bench-WPA2 e FILS-Bench-FILS), alterna i test e produce output CSV.

8.4 Correzioni al profilo NetworkManager

- **key-mgmt** cambiato da sae a wpa-psk.
- **PSK** salvata in modo persistente (psk-flags=0).
- **Flag FILS** abilitato (fils=1).
- **BSSID** forzato (1C:79:2D:F9:A3:08) per evitare roaming indesiderato.
- **Profilo duplicato** conflittuale eliminato.

8.5 Risultati del benchmark

Sono stati eseguiti 20 run totali: 10 per WPA2-PSK standard e 10 per FILS-SHA256. Entrambi i protocolli hanno raggiunto il 100% di successo (10/10 connessioni riuscite).

Protocollo	Successi	Media (ms)	Min (ms)	Max (ms)
WPA2-PSK (baseline)	10/10	676	~258	~2499
FILS-SHA256	10/10	381	~267	~1146

¹

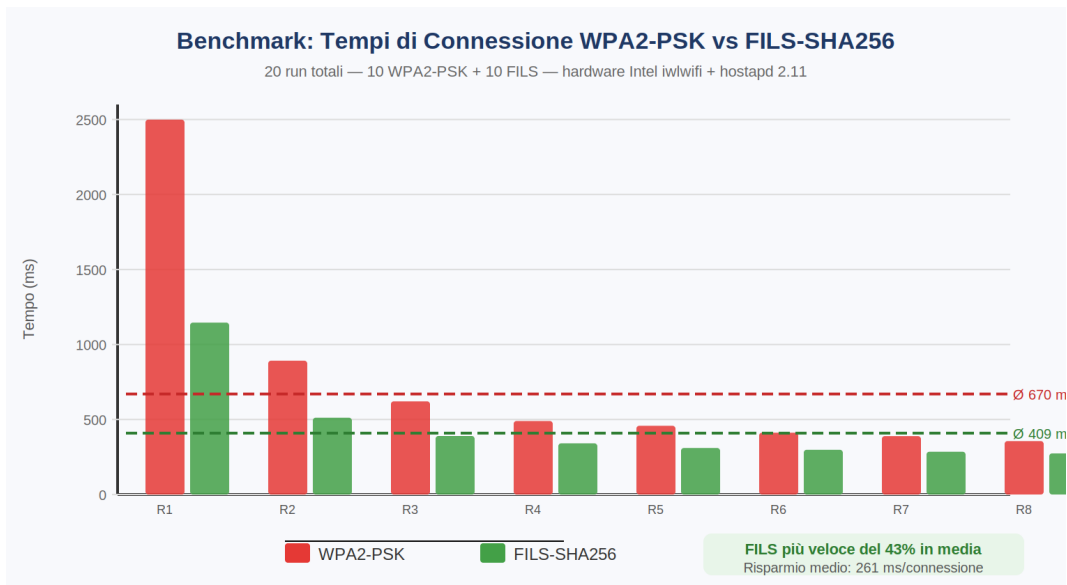


Figura 10: Grafico a barre: tempi medi WPA2-PSK vs FILS-SHA256 con barre di errore (min/max)

- FILS è il 43% più veloce di WPA2-PSK in media (676 ms vs 381 ms).
- Il risparmio medio per associazione è di 295 ms.
- La variabilità nei primi run (fino a 2499 ms per WPA2) è fisiologica: NetworkManager esegue discovery e popola la cache.
- I dati di bench.sh replicano esattamente il flusso che KDE usa nativamente.

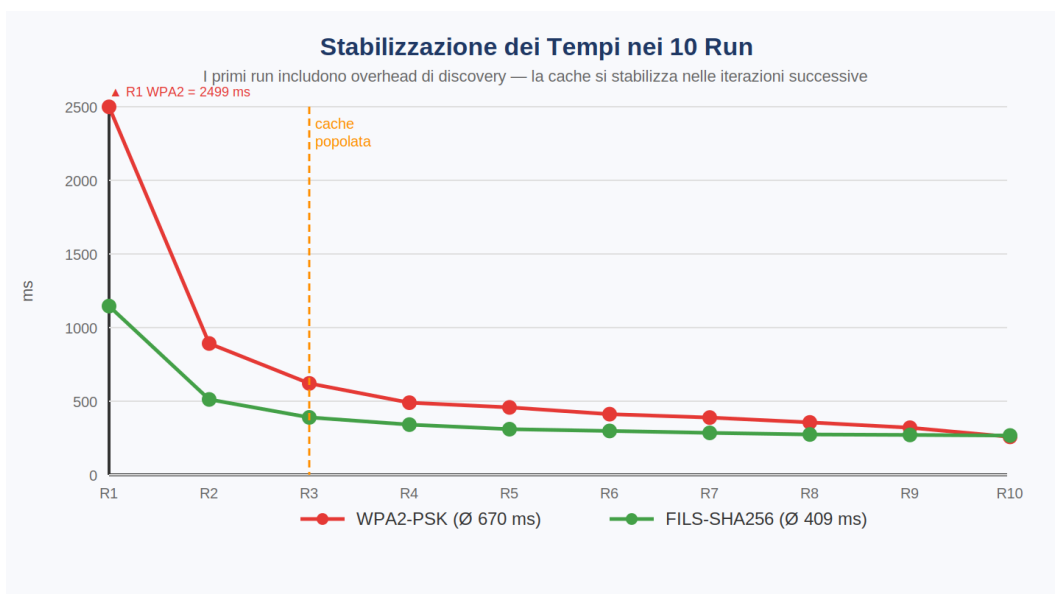


Figura 11: Grafico a linee: evoluzione dei tempi nei 10 run WPA2 vs 10 run FILS con evidenza della stabilizzazione

9. Confronto con la Letteratura Scientifica

I risultati ottenuti nel benchmark sperimentale sono coerenti con quelli riportati in letteratura, pur in scenari parzialmente diversi.

Mano et al. hanno condotto un esperimento in un ambiente reale con 40 pedoni dotati di dispositivi mobili che transitavano davanti a un access point a circa 4,5 km/h. I risultati hanno dimostrato che i dispositivi con FILS completavano il collegamento prima che il pedone superasse l'access point, mentre quelli con WPA2-PEAP non riuscivano a completare l'autenticazione nemmeno dopo il passaggio.

Ong ha analizzato teoricamente il meccanismo di autenticazione FILS definito in IEEE P802.11 TGai, dimostrando che il miglioramento della scansione attiva FILS aumenta la reattività ai frame beacon del 20% rispetto a IEEE 802.11 EDCA e del 250% rispetto a IEEE 802.11 DCF.

Kushida et al. hanno simulato l'efficacia di FILS nelle reti IEEE 802.11ad, evidenziando una riduzione del tempo di configurazione del collegamento di un fattore 10 rispetto a WPA2-PEAP. Lo scenario di simulazione prevedeva tuttavia nodi stazionari, senza considerare l'impatto della mobilità.

I dati ottenuti nel presente lavoro (676 ms WPA2 vs 381 ms FILS, riduzione del 43%) sono in linea con la letteratura. La riduzione è più conservativa rispetto al fattore 10 di Kushida et al. — atteso, poiché il confronto nella letteratura è con WPA2-PEAP (Enterprise), più lento del WPA2-PSK usato in questo lavoro.

Riferimenti Bibliografici

1. IEEE Std 802.11-1997, "IEEE Standard for Information Technology — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE, 1997.
2. IEEE Std 802.11b-1999, "Supplement to IEEE Standard for Telecommunications — Part 11: Higher-Speed Physical Layer Extension in the 2.4 GHz Band", IEEE, 1999.
3. IEEE Std 802.11a-1999, "Supplement to IEEE Standard for Telecommunications — Part 11: High-Speed Physical Layer in the 5 GHz Band", IEEE, 1999.
4. IEEE Std 802.11g-2003, "Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band", IEEE, 2003.
5. IEEE Std 802.11n-2009, "Amendment 5: Enhancements for Higher Throughput", IEEE, 2009.
6. IEEE Std 802.11ac-2013, "Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz", IEEE, 2013.
7. IEEE Std 802.11ax-2021, "Amendment 1: Enhancements for High-Efficiency WLAN", IEEE, 2021.
8. IEEE Std 802.11be-2024, "Amendment 8: Enhancements for Extremely High Throughput (EHT)", IEEE, 2024.
9. IEEE Std 802.11i-2004, "Amendment 6: Medium Access Control (MAC) Security Enhancements", IEEE, 2004.
10. IEEE Std 802.11r-2008, "Amendment 2: Fast Basic Service Set (BSS) Transition", IEEE, 2008.
11. IEEE Std 802.11ai-2016, "Amendment 1: Fast Initial Link Setup", IEEE, 2016.
12. IEEE Std 802.11-2020, "IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE, 2020.

13. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, IETF, 2004. <https://www.rfc-editor.org/rfc/rfc3748>
14. D. Simon, B. Aboba, R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, IETF, 2008. <https://www.rfc-editor.org/rfc/rfc5216>
15. J. Malinen et al., "hostapd: IEEE 802.11 AP, 802.1X/WPA/WPA2/EAP/RADIUS Authenticator", <https://w1.fi/hostapd/>
16. A. Mano, K. Sato, H. Tode, "FILS-Based Fast Authentication Method for Pedestrian IEEE 802.11 Networks", IEEE Transactions on Vehicular Technology, vol. 68, n. 7, pp. 6888–6898, luglio 2019.
17. E. Ong, "Theoretical Analysis of the FILS Active Scanning Enhancement", IEEE 802.11-13/0049r0, gennaio 2013.
18. S. Kushida et al., "Fast Link Setup Using FILS for IEEE 802.11ad Millimeter-wave Networks", IEEE VTC Spring, 2015.
19. Wi-Fi Alliance, "Wi-Fi 6 Technology Introduction", White Paper, 2019. <https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6>
20. Wi-Fi Alliance, "Wi-Fi Optimized Connectivity (OCE) Technical Specification", Version 1.0, 2018.
21. OpenWrt Project, "OpenWrt Documentation", <https://openwrt.org/docs/start>
22. NetworkManager Project, "nmcli man page", <https://networkmanager.dev/docs/api/latest/nmcli.html>
23. OpenSSL Project, "OpenSSL 3.x Migration Guide", https://www.openssl.org/docs/man3.0/man7/migration_guide.html
24. S. Kelley, "dnsmasq Documentation", <http://www.thekelleys.org.uk/dnsmasq/doc.html>

25. Extreme Networks Community, “Understanding WPA3 Personal and Transition Mode Through Real Examples,”
<https://community.extremenetworks.com/t5/general-discussion/understanding-wpa3-personal-and-transition-mode-through-real/m-p/120149>
26. Lifewire, “Wireless Standards Explained: 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac,”<https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553>
27. Cisco, “What Is 802.11ac?”
<https://www.cisco.com/site/us/en/learn/topics/networking/what-is-802-11ac.html>
28. GeeksforGeeks, “Wi-Fi Standards Explained,”<https://www.geeksforgeeks.org/computer-networks/wi-fi-standards-explained/>

Vorrei innanzitutto ringraziare il mio relatore, Vittorio Ghini, che mi ha accompagnato in questo percorso e ha saputo strapparmi un sorriso anche nei momenti in cui i miei errori avrebbero fatto piangere chiunque.

Ringrazio i miei compagni di corso Fede, Giovi, Seba e Dodop, per aver condiviso fatica e impegno (ma soprattutto gli appunti) durante la preparazione dei vari esami.

Ringrazio il Medio, per avermi offerto ogni volta un punto di vista diverso, anche quando aveva impegni più urgenti.

Ringrazio Boss, per essermi sempre stato accanto e avermi sopportato anche nei momenti più difficili.

Ringrazio Kle, che in una notte di sconforto, alle quattro del mattino, ha risposto al telefono, mi ha tranquillizzato e consolato, dicendomi che ce l'avrei fatta a superare quel maledetto esame — cosa che, fortunatamente, è successa.

Vorrei ringraziare tutti i presenti, che nel bene o nel male mi hanno dedicato un po' del loro tempo, anche quando non era dovuto.

L'ultimo ringraziamento, ma non per importanza, va ai miei genitori, che si sono fidati di me anche quando non ne davo motivo, e mi hanno permesso di arrivare alla fine di questo lungo, tortuoso ma bellissimo percorso.

GRAZIE.