Università degli Studi eCampus

Tesi di Laurea

Domotica Residenziale

Evoluzione dei Protocolli di Comunicazione IoT e Gestione di Dispositivi Multimarca

Relatore: Prof. Christian Callegari
Candidato: Michele Rota Biasetti
Matricola nº 1518870

Anno accademico 2024/2025

Indice

Capitolo 1

Introduzione

Negli ultimi anni, le tecnologie legate all'Internet of Things (IoT) hanno trasformato radicalmente il nostro modo di vivere gli spazi domestici. La casa tradizionale, un tempo costituita semplicemente da strutture fisiche e arredi, si è evoluta in un ambiente intelligente e interconnesso, capace di rispondere dinamicamente alle nostre necessità quotidiane attraverso la domotica. Pensiamo ad esempio a quanto sia comodo accendere il riscaldamento mentre si sta tornando a casa dal lavoro, così da trovare la casa già calda e risparmiare anche energia.

Le radici della domotica affondano negli anni '80, quando i primi sistemi cablati, seppur rudimentali come il protocollo X10, permettevano già il controllo remoto di luci ed elettrodomestici. Il decennio successivo ha segnato un'accelerazione significativa: l'introduzione di sistemi più sofisticati come KNX e l'avvento delle reti wireless (Zigbee, Z-Wave) hanno reso la casa intelligente accessibile a tutti. Molti di noi ricordano l'impatto dei primi termostati Nest o delle lampadine Philips Hue, prodotti che hanno fatto capire alle persone comuni quanto può essere utile la domotica in casa.

L'arrivo dell'intelligenza artificiale ha ulteriormente ampliato le possibilità ed accellerato il cambiamento in atto. Oggi le nostre case non si limitano a rispondere ai nostri comandi: è come se ci conoscessero e si adattassero a noi. Per esempio, dopo qualche settimana il sistema capisce che di solito accendiamo le luci del salotto verso le 19:00 e inizia a farlo automaticamente. Gli assistenti vocali come Alexa, Google o Siri non sono più semplici esecutori di ordini: a volte ci sorprendono suggerendo cose utili tipo "Hey, sta per piovere, vuoi che chiuda le finestre?" oppure "È ora di andare a dormire, spengo le luci?". È un po' come avere un maggiordomo digitale che impara a conoscerti giorno dopo giorno.

L'edge computing costituisce un'innovazione particolarmente rilevante, consentendo l'elaborazione dei dati direttamente a livello locale, eliminando la dipendenza dal cloud. Questo approccio migliora sensibilmente i tempi di risposta: una telecamera di sicurezza con capacità di edge computing può identificare immediatamente un intruso e inviare alert in tempo reale, senza dover attendere l'elaborazione su server remoti.

Le tecnologie di rete continuano a evolversi e questo porterà sicuramente nuove possibilità per la casa intelligente. Già oggi vediamo come il miglioramento delle connessioni permetta di controllare i dispositivi con maggiore affidabilità e velocità. Nel prossimo

futuro, potremmo vedere interfacce più intuitive e una maggiore integrazione con servizi esterni. Naturalmente, ogni innovazione porta con sé nuove sfide legate alla sicurezza e alla protezione dei dati personali.

Tuttavia, una delle sfide più rilevanti nel settore della domotica residenziale riguarda l'interoperabilità tra dispositivi di differenti produttori. L'esperienza comune di molti utenti che si approcciano alla domotica nella propria abitazione sono le difficoltà legate alla gestione di applicazioni multiple e protocolli di comunicazione non compatibili, oltre alla necessità di acquisire componenti hardware dedicate per ciascun ecosistema proprietario (Hub per la gestione dei diversi dispositivi per ogni marca). Tuttavia l'introduzione di standard aperti come il protocollo Matter rappresenta un'evoluzione significativa in questa direzione, favorendo una maggiore integrazione tra soluzioni di produttori diversi e la possibilità di avere un unico Hub centrale in grado di gestire dispositivi di marche differenti.

La presente tesi si focalizza sull'evoluzione dei protocolli di comunicazione IoT nella domotica residenziale, con particolare enfasi su sicurezza, prestazioni e interoperabilità. Per concretizzare l'analisi teorica, presenterò un caso studio basato su Apple HomeKit, selezionato per la sua usabilità e le robuste caratteristiche di sicurezza.

1.1 Approccio metodologico

Il lavoro presentato in questa tesi nasce dall'esigenza di comprendere a fondo il mondo della domotica residenziale, combinando diversi punti di vista per offrire una visione il più possibile completa e pratica.

- **Esplorazione della letteratura**: ho consultato numerose pubblicazioni tecniche e articoli specializzati, cercando di selezionare le fonti più recenti e significative per mantenermi aggiornato sugli sviluppi del settore;
- **Confronto tra protocolli**: ho messo a confronto le diverse tecnologie disponibili, basandomi su informazioni pubblicamente accessibili e opinioni di esperti del settore, per capire punti di forza e debolezza di ciascuna soluzione;
- **Osservazione di esempi concreti**: ho dedicato particolare attenzione ai sistemi già presenti sul mercato, con un focus su Apple HomeKit come caso interessante di tecnologia ben integrata nell'esperienza quotidiana degli utenti;
- **Esperienza diretta**: ho avuto modo di sperimentare personalmente con alcuni dispositivi di marche diverse, toccando con mano le sfide che si incontrano quando si cerca di far dialogare prodotti di aziende differenti.

Attraverso questo percorso ho potuto esplorare il mondo della domotica da diverse angolazioni, cercando di capirne pregi e difetti. Lo scopo è offrire spunti pratici e considerazioni concrete a chi vuole iniziare a rendere la propria casa più intelligente, andando oltre la semplice teoria.

1.2 Obiettivi della ricerca

Questa tesi si propone diversi obiettivi, che nascono dalla natura complessa e variegata del mondo della domotica oggi:

- **Analisi evolutiva**: tracciare un quadro completo dell'evoluzione storica e tecnologica dei protocolli IoT nel contesto domotico, evidenziando le forze trainanti del cambiamento e le tendenze emergenti;
- **Valutazione critica della sicurezza**: esaminare approfonditamente le vulnerabilità specifiche dei sistemi IoT domestici, proponendo strategie di mitigazione pratiche semplici e gestibili per l'utente finale;
- **Comparazione prestazionale**: sviluppare una valutazione sistematica delle performance dei protocolli principali attraverso metriche quantitative significative (latenza, throughput, consumo energetico, scalabilità);
- **Studio dell'interoperabilità**: identificare e descrivere strategie concrete per l'integrazione efficace di dispositivi eterogenei, con particolare attenzione alle sfide pratiche di implementazione;
- **Validazione empirica**: fornire un esempio tangibile attraverso l'implementazione pratica con Apple HomeKit, dimostrando l'applicabilità dei principi teorici discussi.

Questo lavoro di tesi è un mix di teoria e pratica, cerca di essere utile sia per chi studia questi argomenti sia per chi vuole semplicemente migliorare la propria casa con la tecnologia.

Capitolo 2

La Domotica Residenziale

Negli ultimi decenni, l'evoluzione delle tecnologie digitali ha profondamente trasformato il nostro modo di vivere la casa, dando origine al concetto di casa intelligente. Questo processo ha permesso che la domotica residenziale sia diventata una realtà tangibile, non più solamente in scenari futuristici o in prototipi sperimentali. L'automazione dei dispositivi domestici, la possibilità di controllarli da remoto e la loro capacità di apprendere dai nostri comportamenti e dalle nostre preferenze, oggi è una realtà presente in molte abitazioni moderne.

La domotica rappresenta una trasformazione a 360 gradi del modo in cui vengpono progettati gli ambienti domestici, vissuti e gestiti, non è solamente un'insieme di gadget tecnologici. Attraverso l'integrazione tra le diverse componenti, sensori, attuatori, interfacce utente e protocolli di comunicazione, l'abitazione si delinea come un ecosistema digitale interconnesso, orientato al miglioramento dell'efficienza energetica, della sicurezza, del comfort e dell'accessibilità.

2.1 Definizione e principi fondamentali

2.1.1 Cos'è davvero la domotica?

Il termine *domotica* è l'unione del termine latino *domus* (casa) e dal termine *informatica*. Indica l'integrazione di tecnologie elettroniche, informatiche e di telecomunicazione per automatizzare, controllare e ottimizzare i sistemi presenti in un'abitazione. Il suo scopo principale è migliorare il comfort, la sicurezza, l'efficienza energetica e l'accessibilità degli ambienti domestici (Wikipedia contributors 2024).

2.1.2 I pilastri della casa intelligente

I principi fondamentali che guidano un sistema domotico efficace ed efficiento sono:

- **Automazione**: la casa esegue azioni senza un intervento diretto da parte dell'abitante della casa, basandosi su orari, sensori o scenari predefiniti;
- **Integrazione**: tutti i dispositivi cooperano in modo sinergico all'interno di un ecosistema condiviso;

- **Personalizzazione**: la casa si adatta alle abitudini, alle preferenze e alle necessità specifiche dei suoi abitanti;
- **Interoperabilità**: i dispositivi dei diversi produttori comunicano tra loro in modo coerente, riducendo frammentazione e complessità.

2.2 Componenti principali di un sistema domotico

Un sistema domotico può essere paragonato ad esempio a un organismo vivente, dove abbiamo i sensori che percepiscono l'ambiente, gli attuatori che compiono le azioni, una rete nervosa che serve per la comunicazione e un cervello centrale che riesce a coordinare il tutto.

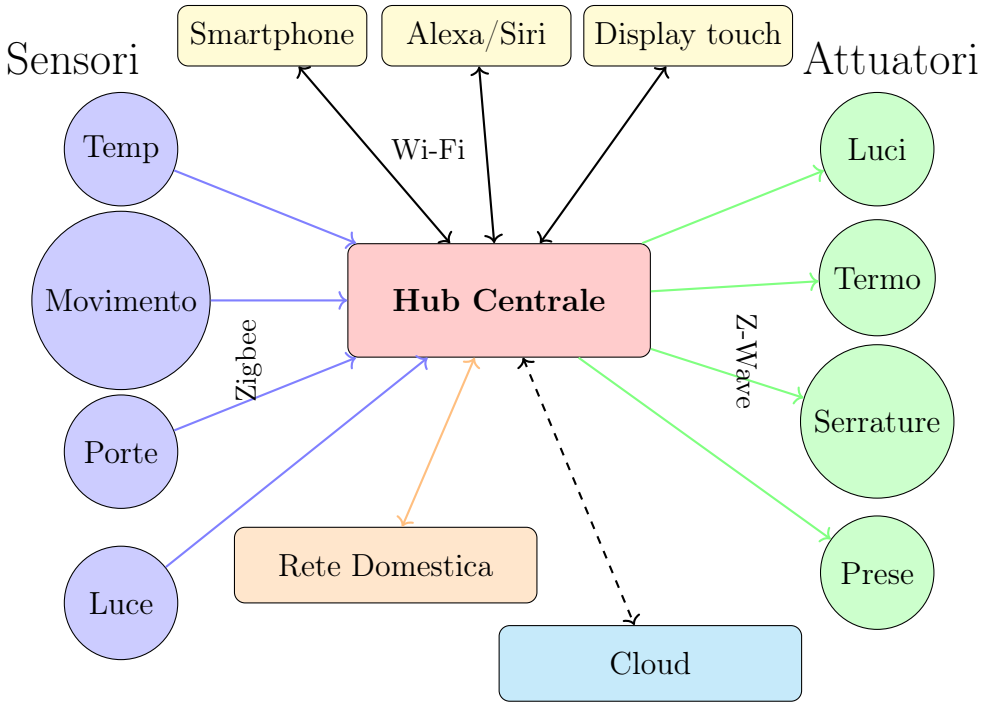

Figura 2.1: Architettura tipica di un sistema domotico residenziale

2.2.1 Sensori

I sensori servono a raccogliere le informazioni sull'ambiente circostante come ad esempio:

- misuratorazione dell'ambiente (per la temperatura, l'umidità, la luminosità, la qualità dell'aria, etc.);
- rilevamento di movimento/presenza (PIR, microonde, ultrasuoni);
- controlli di sicurezza (controllano l'apertura porte/finestre, la presenza di fumo, gas, fuiriuscite di acqua);
- misuratorazione del consumo energetico.

2.2.2 Attuatori

Gli attuatori sono i dispositivi che trasferiscono i comandi ricevuti in azioni fisiche:

- per accensione/spegnimento di luci e dispositivi;
- per il controllo di tapparelle, tende e infissi motorizzati;
- per la regolazione di riscaldamento e condizionamento;
- per la gestione di elettrodomestici e impianti multimediali.

2.2.3 Controller e hub

L'unità centrale (hub) è il vero e proprio cervello del sistema, deve gestire le regole di automazione, interpretare i dati e coordinare le azioni sugli attuatori. In alcuni casi può essere un dispositivo fisico dedicato, un assistente vocale (es. Alexa, Google Home) o un server locale (es. Home Assistant su Raspberry Pi).

2.2.4 Interfacce utente

Gli utenti possono interagire con il sistema tramite:

- App mobili;
- Interfacce vocali;
- Dashboard web;
- Pulsanti intelligenti o pannelli touch.

2.2.5 Reti di comunicazione

La rete collega tutti i dispositivi tra di loro. Può essere cablata (es. KNX) o wireless (es. Zigbee, Z-Wave, Wi-Fi, Thread). I protocolli scelti influenzano la scalabilità, l'efficienza e la sicurezza del sistema.

2.3 Vantaggi della domotica

2.3.1 Efficienza energetica

La domotica consente un uso più consapevole delle risorse energetiche utilizzate nella casa:

- ottimizzazione del riscaldamento e raffrescamento;
- spegnimento automatico di luci e dispositivi inutilizzati;
- monitoraggio dei consumi in tempo reale.

2.3.2 Sicurezza

Grazie all'utilizzo dei sensori e alle automazioni è possibile ricevere notifiche rendendo la casa più sicura:

- rilevamento intrusioni o incidenti (fumo, acqua, CO);
- gestione remota e controllo in tempo reale;
- registrazione video e notifiche intelligenti.

2.3.3 Comfort e accessibilità

L'automazione è alla base per la semplificazione la vita quotidiana:

- scenari personalizzati (es. "buongiorno", "cinema");
- controllo vocale per utenti con disabilità;
- adattamento dinamico dell'ambiente alle esigenze familiari.

2.4 Sfide attuali e prossimi capitoli

Nonostante il progresso tecnologico ed alla riduzione dei costi, persistono però numerosi ostacoli ad un'adozione diffusa:

- **Interoperabilità**: i dispositivi di marche diverse spesso non comunicano bene tra di loro
- **Sicurezza e privacy**: i dispositivi connessi devono proteggere i dati e gli accessi non autorizzati
- **Affidabilità**: un sistema domestico deve funzionare anche in caso di disconnessioni dalla rete o in caso di guasti di alcune sue componenti

Nel prossimo capitolo analizzeremo più da vicino le tecnologie di comunicazione che rendono possibile tutto questo, confrontando protocolli cablati e wireless in termini di prestazioni, consumo e compatibilità.

Capitolo 3

Evoluzione dei Protocolli di Comunicazione IoT

3.1 Introduzione ai protocolli IoT

I protocolli di comunicazione IoT sono il vero e proprio "linguaggio" che permette ai dispositivi intelligenti di casa nostra di parlarsi e collaborare. Pensate a quando accendete la luce dal vostro smartphone o regolate il termostato prima di arrivare a casa, tutto questo è possibile grazie a protocolli che gestiscono la comunicazione tra dispositivi diversi, spesso di marche e tecnologie differenti. Nel tempo, questi protocolli si sono evoluti per rispondere a nuove esigenze, come consumi energetici più bassi, maggiore sicurezza e facilità d'uso. I protocollik possono essere divisi in due grandi famiglie: quelli cablati, come KNX e RS-485, e quelli wireless, come Zigbee, Z-Wave, Wi-Fi, Bluetooth Low Energy, Thread e Matter.

3.2 Protocolli cablati: KNX e RS-485

I protocolli cablati sono stati i pionieri della domotica e ancora oggi sono molto usati, soprattutto in contesti dove la stabilità della comunicazione è fondamentale.

KNX è uno standard internazionale molto affidabile e flessibile. Immaginate un grande edificio, come un hotel o un ufficio, dove luci, riscaldamento, tende e sistemi di sicurezza devono funzionare in modo coordinato e senza intoppi. KNX permette di collegare tutti questi dispositivi con un unico sistema cablato, garantendo che tutto funzioni senza problemi. Il vantaggio principale nel suo utilizzo è la grande affidabilità e la possibilità di personalizzare il sistema in base alle esigenze specifiche in fase di progettazione. Tuttavia, l'installazione richiede un intervento tecnico specializzato e può risultare costosa, il che lo rende meno adatto per case più piccole, inoltre successive modifiche o ampliamenti non previsti richiedono nuovi lavori sull'infrastruttura della casa.

RS-485, invece, è spesso usato in contesti industriali o in impianti domestici più semplici per risolvere specifici problemi, come ad esempio un sistema di allarme o controllo degli accessi. RS-485 può garantire una comunicazione stabile anche su lunghe distanze e in ambienti con molte interferenze elettriche, questo si traduce in un sistema robusto che

raramente perde il segnale. Tuttavia, come KNX, richiede cablaggi e competenze tecniche per l'installazione, inoltre ache in questo caso sono onerosi i successivi ampliamenti e modifiche se non previste nella prima fase di progettazione.

3.3 Protocolli wireless: Zigbee, Z-Wave, Wi-Fi e Bluetooth Low Energy

Con l'avvento delle tecnologie wireless, la domotica è diventata più accessibile e flessibile, permettendo installazioni più semplici e meno invasive.

Zigbee è molto popolare per dispositivi come sensori di movimento, termostati smart e lampadine intelligenti. Ad esempio, in una casa, i sensori Zigbee possono comunicare tra loro formando una rete mesh, se un dispositivo è lontano dal router il segnale passa attraverso altri dispositivi fino a raggiungerlo. Questa tecnica permette di poter installare anche in case di grandi dimensioni o con muri spessi che schermerebbero il segnale, diversi dispositivi. Un vantaggio è che la comunicazione tra i dispositivi e l'hub centrale resta stabile, a questo si aggiunge il basso consumo energetico, che permette ai sensori di durare anni con una singola batteria. Lo svantaggio è la necessità di un hub centrale per ogni marca di dispositivi e la difficoltà nella configurazione e nei successivi momenti di aggiornamento del firmware dei singoli dispositivi.

Z-Wave è simile a Zigbee ma spesso preferito in ambito residenziale per la sua semplicità di configurazione iniziale, i wizard di installazione e configurazione sono intuitivi e permettono di collegare dispositivi come serrature smart o controller per tapparelle. Un'ulteriore caratteristica è la sicurezza integrata, così come la compatibilità tra marche diverse, tuttavia, la velocità di trasmissione è limitata rispetto al Wi-Fi, il che lo rende meno adatto a trasmettere grandi quantità di dati.

Wi-Fi è probabilmente il protocollo più familiare, essendo quello usato per connettere smartphone, computer e smart TV a internet, molti dispositivi IoT, come videocamere di sicurezza o assistenti vocali, usano il Wi-Fi perché garantisce alta velocità e non richiede hub aggiuntivi. Lo svantaggio principale sta nell'alto consumo energetico, che limita l'uso di Wi-Fi in dispositivi alimentati a batteria, altre problematiche riguradano la sicurezza di questi dispositivi e la congestione della rete wi-fi domestica.

Bluetooth Low Energy (BLE) è ideale per dispositivi a corto raggio e a bassissimo consumo, come smartwatch, fitness tracker o sensori di prossimità. Un utilizzo molto comune di questo protocolo è per sbloccare la porta o accessi quando si avvicina uno smartphone od un Tag BLE. Il vantaggio è il risparmio energetico e la semplicità, ma la portata limitata lo rende inadatto per coprire tutta la casa senza dispositivi aggiuntivi.

3.4 Thread e Matter: verso l'interoperabilità e l'unificazione

Chi si avvicina alla domotica spesso scopre con disappunto che i dispositivi di marche diverse faticano a comunicare tra loro. È frustrante comprare una lampadina smart di un brand e scoprire che non funziona con l'hub di un altro. Thread e Matter sono protocolli nati proprio per risolvere questa babele tecnologica.

Thread è una rete mesh basata su IPv6 che permette ai dispositivi di comunicare direttamente tra loro senza passare per un hub centrale. In pratica, le luci, i sensori e i termostati si collegano tra loro creando una ragnatela di connessioni: se una lampadina si spegne o perde il segnale, gli altri dispositivi trovano automaticamente percorsi alternativi per comunicare. Il risultato? Una rete che si auto-ripara e funziona con maggiore stabilità rispetto a tecnologie precedenti come Zigbee o Z-Wave. La configurazione è generalmente più semplice e immediata. Il rovescio della medaglia è che Thread è ancora una tecnologia giovane e non tutti i prodotti sul mercato la supportano ancora.

Matter rappresenta l'iniziativa più ambiziosa nel settore della domotica, concepita per stabilire un protocollo di comunicazione universale tra dispositivi intelligenti di differenti produttori. Questo standard si propone di risolvere le problematiche di interoperabilità che caratterizzano l'attuale panorama della smart home, dove dispositivi appartenenti a ecosistemi diversi presentano significative limitazioni nell'integrazione reciproca. L'implementazione di Matter consente ai dispositivi certificati di operare trasversalmente su piattaforme multiple, includendo i principali ecosistemi commerciali, tale standardizzazione favorisce una maggiore flessibilità nella composizione dei sistemi domotici, permettendo scelte basate su criteri qualitativi e funzionali piuttosto che su vincoli di compatibilità.

Nonostante le promettenti prospettive, l'adozione del protocollo si trova ancora in fase di espansione, con una progressiva ma non ancora completa diffusione nel mercato. È importante sottolineare che il protocollo Matter non consente l'integrazione di qualsiasi tipologia di dispositivo, ma definisce specifiche categorie supportate attraverso le proprie direttive tecniche. Questo approccio selettivo garantisce l'affidabilità e la coerenza dell'ecosistema, limitando tuttavia l'universalità inizialmente prospettata.

3.5 Criteri di selezione dei protocolli

Quando si deve scegliere un protocollo per la casa intelligente, bisogna considerare diversi aspetti pratici:

- **Consumo energetico**: Se avete dispositivi alimentati a batteria, come sensori o serrature, è fondamentale scegliere protocolli a basso consumo per evitare continui cambi di batteria.
- **Portata e copertura**: In case grandi o con muri spessi, protocolli con rete mesh come Zigbee, Thread o Z-Wave possono garantire una copertura migliore.
- **Velocità e latenza**: Per applicazioni che richiedono risposte immediate, come videocamere o sistemi di allarme, è meglio optare per protocolli veloci come Wi-Fi.

- **Facilità d'uso e integrazione**: Per far funzionare insieme dispositivi di produttori diversi, è essenziale verificare che supportino gli stessi protocolli di comunicazione, preferendo standard aperti che facilitino la configurazione e garantiscano una reale interoperabilità.
- **Sicurezza e privacy**: Proteggere la propria rete domestica è fondamentale, quindi è bene preferire protocolli che offrono solide misure di sicurezza.

Nel prossimo capitolo approfondiremo proprio questi aspetti di sicurezza e privacy nei protocolli IoT domestici, fornendo consigli pratici per mantenere la vostra casa intelligente protetta e affidabile.

Capitolo 4

Sicurezza e Privacy nella Domotica Residenziale

4.1 Introduzione alla sicurezza IoT domestica

La tecnologia ha reso le nostre case più comode e facili da gestire: dal riscaldamento controllato a distanza alle luci che si regolano da sole. Ma insieme a questi benefici ci sono anche aspetti meno visibili, come la grande quantità di dati personali che questi sistemi raccolgono e trattano ogni giorno.

È interessante riflettere sulla quantità di informazioni che fluiscono attraverso una casa intelligente: orari di presenza, preferenze climatiche, abitudini di illuminazione, fino ad arrivare ai dati biometrici raccolti dalle telecamere di ultima generazione. Ogni componente del sistema - dal termostato intelligente all'assistente vocale - rappresenta contemporaneamente un'opportunità e una potenziale vulnerabilità.

Ogni nuovo dispositivo connesso aggiunge un "punto d'ingresso" alla nostra rete domestica. Non dobbiamo più pensare alla sicurezza di un solo apparecchio, ma di un sistema dove tutto comunica con tutto, spesso anche con servizi online. Questa rete invisibile all'occhio dell'utente richiede strategie di protezione completamente riviste.

L'approccio più efficace prevede l'integrazione della sicurezza fin dalle fasi iniziali di progettazione - il cosiddetto principio del *security by design*. Questo significa implementare protezioni a più livelli: cifratura dei dati in transito e a riposo, gestione granulare dei permessi, meccanismi di difesa adattivi capaci di rispondere a minacce in evoluzione.

4.2 Minacce e vulnerabilità comuni

Le minacce alla domotica hanno dinamiche tutte loro, diverse da quelle della sicurezza informatica "classica". Capire queste differenze è il primo passo per proteggere davvero la propria casa smart.

4.2.1 Intrusioni e accessi non autorizzati

Un aspetto sorprendentemente critico riguarda la presenza di credenziali di default nei dispositivi IoT che non vengono aggiornate. Nonostante anni di sensibilizzazione, nume-

rosi produttori continuano a distribuire dispositivi con combinazioni username/password facilmente reperibili attraverso una semplice ricerca online. Questa pratica, unita alla tendenza degli utenti a non modificare tali credenziali, crea vulnerabilità immediate e facilmente sfruttabili.

La situazione è aggravata dalla mancanza di meccanismi che obblighino l'utente a personalizzare le credenziali al primo utilizzo - una misura semplice che potrebbe eliminare gran parte di questi rischi.

4.2.2 Malware specifici per dispositivi embedded

I dispositivi IoT, caratterizzati da risorse computazionali limitate e sistemi operativi minimali, presentano un profilo di vulnerabilità unico. I malware progettati per questi ambienti sfruttano proprio queste limitazioni: la scarsa capacità di implementare antivirus tradizionali, l'impossibilità di monitorare in tempo reale i processi in esecuzione, la difficoltà nell'applicare patch di sicurezza.

Questi software malevoli possono operare inosservati per periodi prolungati, trasformando dispositivi apparentemente innocui in strumenti per la raccolta di dati sensibili o in nodi di botnet per attacchi distribuiti.

4.2.3 Vulnerabilità nei protocolli di comunicazione

L'eterogeneità dei protocolli wireless nella domotica - ZigBee, Z-Wave, Wi-Fi, Bluetooth - introduce sfide specifiche di sicurezza. Gli attacchi di tipo Man-in-the-Middle rappresentano una minaccia particolarmente insidiosa in questo contesto. Un attore malevolo può posizionarsi nel percorso di comunicazione tra dispositivi, intercettando e potenzialmente alterando i comandi trasmessi. Consideriamo l'esempio di una serratura intelligente: l'intercettazione dei segnali di controllo potrebbe permettere l'apertura della casa in un secondo momento.

4.2.4 Il caso Mirai: una lezione da non dimenticare

L'epidemia del botnet Mirai nel 2016 rimane un caso di studio fondamentale per comprendere le vulnerabilità sistemiche dell'IoT. Questo malware ha dimostrato come la combinazione di credenziali predefinite e mancanza di aggiornamenti di sicurezza possa trasformare centinaia di migliaia di dispositivi domestici in armi per attacchi DDoS di scala globale. La semplicità dell'attacco - basato essenzialmente sul tentativo sistematico di credenziali note - evidenzia come problemi apparentemente banali possano avere conseguenze devastanti (Antonakakis, April e Bailey 2017).

4.3 Best practice per garantire sicurezza e privacy

Per difendere un ambiente domotico serve una strategia a più livelli, che unisca soluzioni tecniche, buone pratiche e formazione degli utenti. Insieme, questi elementi creano un sistema capace di reagire e adattarsi ai rischi che cambiano nel tempo.

4.3.1 Aggiornamenti e patch management

La gestione sistematica degli aggiornamenti rappresenta la prima linea di difesa contro vulnerabilità note. Questo processo, apparentemente semplice, presenta sfide pratiche significative nell'ambito IoT: molti dispositivi non implementano meccanismi di aggiornamento automatico, richiedendo interventi manuali periodici. La creazione di una routine di verifica - magari calendarizzata mensilmente - può trasformare questa attività da sporadica emergenza a pratica consolidata.

4.3.2 Segmentazione della rete

L'isolamento logico dei dispositivi attraverso la segmentazione di rete offre benefici significativi con un impegno implementativo relativamente contenuto:

- **Rete principale protetta**: riservata a dispositivi contenenti dati sensibili e sistemi IoT verificati
- **Rete ospiti isolata**: per visitatori occasionali, impedendo accessi non autorizzati all'infrastruttura principale

Questa separazione limita la propagazione di eventuali compromissioni e facilita il monitoraggio del traffico anomalo.

4.3.3 Firewall e sistemi di monitoraggio

I router consumer moderni hanno fatto passi significativi nell'integrazione di funzionalità di sicurezza precedentemente riservate ad ambienti enterprise. Produttori come ASUS, Netgear e AVM (Fritz!Box) offrono oggi:

- Sistemi di prevenzione delle intrusioni (IPS) integrati
- Analisi comportamentale del traffico di rete
- Filtri per contenuti malevoli aggiornati in tempo reale
- Sistemi di notifica per eventi di sicurezza rilevanti

L'attivazione di queste funzionalità, spesso disponibili ma disabilitate di default, può incrementare significativamente il livello di protezione con uno sforzo minimo. Alcuni provider hanno iniziato a fornire dispositivi preconfigurati con queste protezioni attive, semplificando ulteriormente l'adozione.

4.3.4 Gestione degli accessi e autenticazione forte

L'implementazione di politiche di accesso robuste richiede un bilanciamento tra sicurezza e usabilità:

- **Principio del privilegio minimo**: assegnare solo i permessi strettamente necessari per ogni utente o dispositivo

- **Autenticazione multi-fattore (MFA)**: integrare fattori di autenticazione aggiuntivi, bilanciando sicurezza e praticità d'uso
- **Gestione centralizzata delle credenziali**: l'utilizzo di password manager facilita l'adozione di credenziali complesse e uniche
- **Rotazione programmata**: stabilire intervalli regolari per l'aggiornamento delle credenziali critiche

4.3.5 Educazione e consapevolezza degli utenti

La componente umana rimane fondamentale in qualsiasi strategia di sicurezza. La formazione degli abitanti della casa, soprattutto per gli utenti con ruoli di gestione amministartiva dei dispositivi, dovrebbe coprire:

- Riconoscimento di tentativi di phishing specifici per dispositivi IoT
- Comprensione dell'importanza degli aggiornamenti di sicurezza
- Capacità di verificare l'autenticità di app e servizi collegati
- Identificazione di comportamenti anomali nei dispositivi

Sessioni informative periodiche, magari integrate con esempi pratici e simulazioni, possono trasformare ogni membro della famiglia in un elemento attivo del sistema di sicurezza.

4.4 Tecniche di crittografia e autenticazione nei protocolli IoT

L'implementazione di meccanismi crittografici in ambienti con risorse limitate rappresenta una delle sfide tecniche più interessanti della sicurezza IoT.

4.4.1 Crittografia end-to-end nei sistemi domotici

La protezione crittografica dei dati deve essere garantita lungo l'intero percorso di trasmissione, dal dispositivo Ioy fino al nostro smartphone. Le limitazioni hardware dei dispositivi IoT impongono scelte oculate nell'implementazione:

- **AES-128**: uno degli standard più diffusi, usato perché offre un buon equilibrio tra sicurezza e velocità. Protegge bene senza pesare troppo sulle prestazioni o sulla batteria.
- **Crittografia a curve ellittiche (ECC)**: garantisce lo stesso livello di protezione di altri sistemi ma con chiavi più corte, quindi più veloce e adatta anche ai dispositivi più piccoli.
- **Suite crittografiche leggere**: algoritmi come ChaCha20-Poly1305, pensati apposta per l'IoT, che mantengono alta la sicurezza anche su hardware con risorse limitate.

4.4.2 Protocolli di comunicazione sicura

L'adattamento dei protocolli di sicurezza tradizionali alle necessità e caratteristiche dei dispositivi IoT ha prodotto soluzioni innovative:

- **DTLS (Datagram TLS)**: una versione di TLS pensata per funzionare bene con il protocollo UDP, utile per dispositivi che si connettono in modo intermittente o con reti non stabili.
- **Protocolli sicuri a livello applicativo**: come CoAP-DTLS e MQTT-TLS, che integrano le funzioni di sicurezza direttamente nel protocollo usato dai dispositivi per comunicare.
- **Meccanismi di attestazione**: sistemi che controllano l'integrità e l'autenticità del dispositivo prima di consentire lo scambio di dati, così da evitare comunicazioni con unità compromesse.

4.4.3 Standard di autenticazione nell'era IoT

La convergenza verso standard aperti facilita l'interoperabilità dei dispositivi di produttori differenti senza compromettere la sicurezza:

- **OAuth 2.0 e OpenID Connect**: permettono di concedere permessi specifici a un servizio senza dover condividere direttamente la password, aumentando la sicurezza.
- **JWT e CBOR Web Tokens**: piccoli "pacchetti" di informazioni firmati digitalmente che contengono tutto ciò che serve per l'autenticazione, riducendo la necessità di mantenere dati lato server.
- **FIDO2/WebAuthn**: sistemi di autenticazione senza password, che usano metodi come impronte digitali o riconoscimento facciale, sempre più adottati anche nei dispositivi IoT.

La selezione di dispositivi che implementano questi standard non solo garantisce maggiore sicurezza ma anche migliore integrazione futura.

4.5 Analisi di casi di violazione della sicurezza in ambito domestico

L'esame di incidenti reali fornisce informazioni preziose per la prevenzione di future compromissioni.

4.5.1 Il caso delle telecamere IP compromesse

L'incidente del 2020 che ha esposto migliaia di feed video domestici rappresenta un caso emblematico e su vasta scala:

- Persistenza di credenziali di accesso di default

- Nessun aggiornamento del firmware da diversi anni
- Esposizione diretta delle porte di gestione dei servizi critici direttamente su Internet
- Assenza di cifratura per lo stream dei video

L'analisi successiva ha rivelato come la concatenazione di vulnerabilità apparentemente minori possa creare brecce di sicurezza maggiori.

4.5.2 L'incidente Ring e le implicazioni sulla privacy

Il caso Ring del 2019 ha evidenziato come la sicurezza debba estendersi oltre il dispositivo stesso. Gli hacker hanno sfruttato diversi punti di vulnerabiltà:

- Riutilizzo di credenziali compromesse in precedenti data breach per lo stesso account personale
- Mancata adozione di MFA nonostante fosse disponibile
- Scarsa attenzione degli utenti agli indicatori di compromissione

La risposta di Amazon - rendere obbligatoria l'autenticazione a due fattori dopo l'azione legale collettiva - dimostra come la pressione regolatoria e sociale possa accelerare l'adozione di misure di sicurezza basilari ma efficaci.

4.5.3 Lezioni apprese e raccomandazioni

L'analisi trasversale di questi incidenti rivela pattern ricorrenti:

1. **Security by default**: la configurazione sicura deve essere lo stato iniziale, non un'opzione
2. **Trasparenza proattiva**: gli utenti devono comprendere quali dati vengono raccolti e come vengono protetti
3. **Modello di responsabilità condivisa**: successo richiede collaborazione tra produttori, provider e utenti finali
4. **Resilienza operativa**: piani di incident response testati minimizzano l'impatto di eventuali breach

4.6 Conclusioni e prospettive future

In ambito domotico, la sicurezza va vista come un processo in continua evoluzione. Ogni progresso tecnologico porta con sé nuove opportunità, ma anche rischi che richiedono un aggiornamento costante delle strategie di difesa.

Le direzioni future più promettenti includono:

- **Intelligenza artificiale per la sicurezza adattiva**: sistemi che apprendono pattern comportamentali per identificare anomalie in tempo reale

- **Tecnologie distributed ledger**: blockchain e simili per garantire integrità e non ripudiabilità dei dati IoT
- **Crittografia post-quantistica**: preparazione proattiva all'era del quantum computing

Vogliamo abitazioni intelligenti che offrano tutti i vantaggi della tecnologia, ma senza sacrificare la sicurezza e la riservatezza dei dati e l'usabilità dei dispositivi. E' un traguardo possibile grazie all'adozione di pratiche consolidate, all'uso di consapevole di soluzioni innovative per la sicurezza e alla formazione continua di chi le utilizza.

Capitolo 5

Analisi delle Prestazioni e Affidabilità dei Protocolli

5.1 Introduzione

Nel contesto della domotica residenziale, la selezione del protocollo di comunicazione rappresenta un passaggio cruciale, capace di incidere in modo determinante sulle prestazioni complessive del sistema, sull'affidabilità delle connessioni tra i dispositivi e, non da ultimo, sull'esperienza d'uso percepita dagli utenti finali. Questo capitolo si propone di esplorare in modo approfondito le caratteristiche tecniche e operative dei principali protocolli IoT impiegati in ambito domestico, offrendo strumenti concreti per orientare la scelta verso la soluzione più adeguata in funzione delle specifiche esigenze progettuali.

L'evoluzione tecnologica degli ultimi anni ha favorito la diffusione di una molteplicità di protocolli, ciascuno sviluppato per rispondere a determinati requisiti funzionali o vincoli strutturali. Nessuno di essi può essere considerato intrinsecamente "migliore" in senso assoluto: la decisione finale deve necessariamente derivare da un'attenta analisi comparativa, che tenga conto di fattori quali la scalabilità, il consumo energetico, la latenza, la sicurezza, la compatibilità con ecosistemi preesistenti e il grado di complessità richiesto per l'integrazione.

5.2 Indicatori chiave di performance

Per capire davvero quanto un protocollo di comunicazione IoT sia efficace all'interno di un'abitazione intelligente, non basta leggerne le specifiche tecniche ma è fondamentale considerare alcuni indicatori chiave di performance, definiti con il nome Key Performance Indicators abbrteviato in (KPI), questi indicatori oggettivi ci aiutano a valutare in modo concreto e comparabile il comportamento di ciascuna tecnologia nelle situazioni reali di abitazioni comuni.

5.2.1 Latenza: il tempo di risposta del sistema

Uno degli aspetti che più influisce sull'esperienza d'uso quotidiana è la **latenza**, ovvero il tempo che passa tra l'invio di un comando e la sua esecuzione. In altre parole,

quanto velocemente la casa "risponde" quando chiediamo qualcosa. È un po' come premere l'interruttore della luce: se dopo averlo fatto ci vogliono più di 200-300 millisecondi perché la lampada si accenda, la sensazione immediata è che qualcosa non funzioni a dovere – anche se tecnicamente tutto è sotto controllo. Questo breve ritardo può sembrare irrilevante, ma oltre una certa soglia diventa fastidioso e può minare la fiducia nel sistema.

Naturalmente, non tutti i protocolli si comportano allo stesso modo. **Zigbee**, ad esempio, è generalmente molto reattivo nelle comunicazioni dirette, con latenze comprese tra i 15 e i 30 millisecondi. Tuttavia, quando la rete diventa più complessa, come nel caso di una struttura mesh con più passaggi intermedi (i cosiddetti multi-hop), il tempo di risposta può allungarsi fino a 50-100 millisecondi.

Il **Wi-Fi**, se ottimizzato per applicazioni in tempo reale, può offrire prestazioni ancora migliori, arrivando a latenze inferiori ai 10 millisecondi. Ma c'è un prezzo da pagare: questi risultati richiedono un consumo energetico decisamente più elevato, rendendo il Wi-Fi meno adatto per dispositivi alimentati a batteria, come sensori o piccoli attuatori che devono funzionare per anni senza manutenzione.

In definitiva, la scelta del protocollo deve sempre tenere conto di un equilibrio tra velocità, efficienza energetica e caratteristiche dell'ambiente domestico in cui verrà implementato. La reattività è importante, ma lo è altrettanto la capacità del sistema di durare nel tempo senza interventi continui.

5.2.2 Consumo energetico: la sfida dell'autonomia

Tra le principali sfide dell'Internet of Things applicato alla domotica, il consumo energetico occupa un ruolo di primo piano. In particolare, numerosi dispositivi domestici, come sensori di movimento, di temperatura, o di apertura porte e finestre, devono poter funzionare per lunghi periodi, spesso per anni, con una singola batteria di piccole dimensioni. In questo scenario, l'efficienza energetica non rappresenta solo un vantaggio, ma un requisito fondamentale per garantire la sostenibilità e l'affidabilità dell'intero ecosistema smart.

I protocolli di comunicazione IoT si distinguono nettamente per quanto riguarda l'impatto energetico, in funzione del loro design, delle modalità di trasmissione e della gestione dei cicli di attività e standby. Di seguito, una panoramica comparativa delle principali soluzioni:

- **Z-Wave**: Progettato fin dalle origini per applicazioni a basso consumo, Z-Wave offre consumi estremamente contenuti in modalità standby (inferiori a 1 µA) e una richiesta energetica in trasmissione intorno ai 30–40 mA, limitata a brevi istanti. Queste caratteristiche lo rendono ideale per dispositivi alimentati a batteria.

- **Zigbee**: Anch'esso particolarmente efficiente, Zigbee utilizza modalità "sleep" avanzate con assorbimenti inferiori ai 3 µA. Il tempo di riattivazione è molto contenuto (meno di 15 ms), garantendo un buon compromesso tra reattività e risparmio energetico.

- **Thread**: Questo protocollo eredita l'approccio efficiente di Zigbee, ma introduce ulteriori ottimizzazioni per supportare il routing basato su IPv6, consentendo

una gestione energetica ancora più flessibile e scalabile, pur mantenendo consumi contenuti.

- **Wi-Fi**: Tradizionalmente meno adatto ai dispositivi a basso consumo, anche nelle sue versioni più recenti – come Wi-Fi 6 – continua a presentare assorbimenti elevati, con consumi in standby nell'ordine dei millesimi di ampere (mA), decisamente superiori rispetto agli standard sopra citati.

Per rendere il confronto più concreto, si consideri un sensore di temperatura basato su Z-Wave, configurato per trasmettere dati ogni 5 minuti: in condizioni ottimali, può operare per un periodo compreso tra i 5 e i 7 anni con una singola batteria tipo CR2032. Al contrario, un dispositivo Wi-Fi equivalente richiederebbe una ricarica mensile o un'alimentazione continua, fattore che limita fortemente la sua applicabilità in scenari stand-alone.

5.2.3 Larghezza di banda: quanto possono davvero "parlare" i dispositivi

Un altro parametro importante da considerare, soprattutto in certi scenari, è la **larghezza di banda**, ovvero la quantità di dati che possono essere trasmessi attraverso la rete in un dato intervallo di tempo. Anche se molti dispositivi domotici scambiano solo piccoli pacchetti di dati (ad esempio, un comando on/off o la lettura di un sensore), esistono casi d'uso che richiedono una capacità di trasferimento ben più ampia.

Alcuni esempi includono:

- Lo *streaming video* in tempo reale da telecamere di sicurezza
- Gli *aggiornamenti firmware over-the-air*, fondamentali per la manutenzione remota
- Il trasferimento di *log diagnostici* da dispositivi complessi
- Il controllo e la sincronizzazione di *impianti audio multi-room*

In questi contesti, la banda disponibile fa la differenza. I protocolli IoT presentano valori molto diversi in termini di velocità massima e throughput reale, come evidenziato nella tabella seguente:

Protocollo	**Velocità massima**	**Throughput reale stimato**
Z-Wave	100 kbps	40–60 kbps
Zigbee	250 kbps	100–150 kbps
Thread	250 kbps	100–150 kbps
Wi-Fi 4	600 Mbps	100–200 Mbps
Wi-Fi 6	9.6 Gbps	1–2 Gbps

Tabella 5.1: Confronto tra velocità teoriche e throughput pratico dei principali protocolli IoT

Come si osserva, **Wi-Fi** domina nettamente per capacità di banda. Tuttavia, nella maggior parte degli impianti domotici, questa potenza risulta sovradimensionata: un semplice comando per accendere una luce o inviare una lettura della temperatura richiede

pochi byte, rendendo il Wi-Fi inefficiente in termini energetici per compiti così semplici W.-F. Alliance 2022.

In altre parole, usare il Wi-Fi per trasmettere dati minimi è come utilizzare un camion per consegnare una cartolina: funziona, ma è chiaramente uno spreco.

5.2.4 Affidabilità e resilienza: quando la rete deve sapersela cavare da sola

Perché un sistema domotico possa davvero definirsi affidabile, non basta che funzioni "quando tutto va bene": deve essere in grado di reagire e adattarsi anche quando qualcosa non va come previsto. È in queste situazioni che entrano in gioco due concetti fondamentali: **affidabilità** e **resilienza**.

In termini pratici, un protocollo di comunicazione deve possedere alcune capacità essenziali:

- **Gestione delle interferenze**: saper mantenere la comunicazione anche in ambienti ricchi di segnali wireless (Wi-Fi, Bluetooth, ecc.)
- **Ritrasmissione automatica**: garantire che i pacchetti persi vengano inviati di nuovo senza necessità di intervento
- **Routing dinamico**: trovare percorsi alternativi se un nodo della rete diventa inattivo o instabile
- **Prioritizzazione del traffico**: assegnare maggiore importanza ai messaggi critici tramite meccanismi di *Quality of Service* (QoS)

Le reti *mesh* basate su **Zigbee** e **Thread** sono progettate proprio per affrontare queste sfide: grazie ad algoritmi di routing intelligente, sono in grado di riorganizzarsi in autonomia e reindirizzare i messaggi qualora un dispositivo venga rimosso, sostituito o risulti non raggiungibile C. S. Alliance 2024; Group 2023. Questo approccio rende il sistema più flessibile e robusto nel tempo.

Anche **Z-Wave**, pur avendo una struttura mesh meno estesa, offre un vantaggio rilevante: opera su frequenze **sub-GHz**, in particolare intorno agli 868 MHz in Europa, una banda meno affollata rispetto alla classica 2.4 GHz utilizzata da molti altri protocolli. Ciò si traduce in una maggiore immunità alle interferenze, che spesso rappresentano un problema negli ambienti domestici saturi di dispositivi wireless Z.-W. Alliance 2023.

Per quanto riguarda il **Wi-Fi**, nonostante la sua ampia diffusione e le elevate prestazioni in termini di velocità, si dimostra talvolta meno resiliente in ambienti particolarmente congestionati. La stabilità complessiva della rete Wi-Fi dipende fortemente dalla qualità dell'infrastruttura (router, access point, gestione dei canali), e in caso di sovraccarico o malfunzionamenti può mostrare latenze elevate o perdita di pacchetti W.-F. Alliance 2022.

Come illustrato nella Figura 5.1, le reti mesh consentono a ogni nodo di fungere da ponte per altri dispositivi, garantendo comunicazione anche in caso di guasti o disconnessioni.

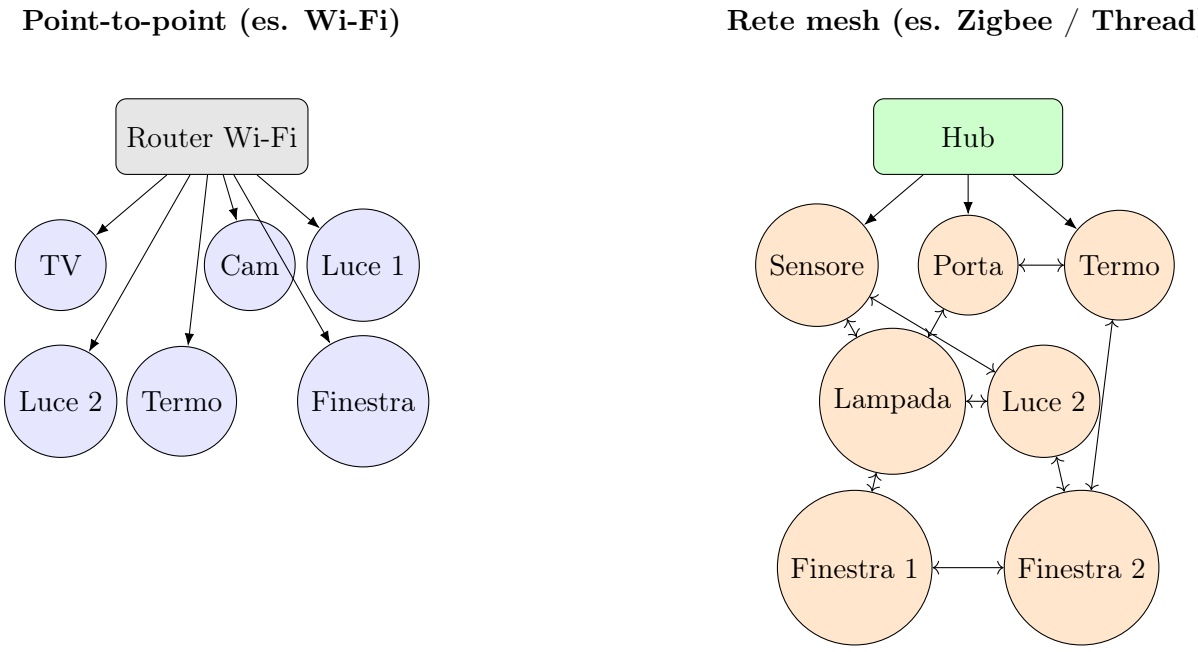

Figura 5.1: Confronto tra rete point-to-point (Wi-Fi) e rete mesh (Zigbee/Thread).

In definitiva, quando si progettano sistemi domotici destinati a durare nel tempo e ad adattarsi a contesti mutevoli, scegliere protocolli con meccanismi di recupero e adattamento diventa una garanzia di stabilità e continuità.

5.3 Confronto prestazionale tra Zigbee, Z-Wave, Wi-Fi, Thread e Matter

5.3.1 Zigbee: il veterano delle reti mesh

Zigbee è considerato uno dei protocolli più consolidati nell'ambito della domotica, grazie alla sua lunga presenza sul mercato e alla vasta adozione da parte dei produttori. Basato sullo standard IEEE 802.15.4, opera principalmente sulla banda a 2.4 GHz, la stessa condivisa con Wi-Fi e Bluetooth.

Punti di forza:

- Ecosistema maturo con ampia disponibilità di dispositivi
- Supporto per reti mesh auto-riparanti fino a 65.000 nodi teorici
- Profili applicativi standardizzati (es. Zigbee Home Automation, Zigbee Light Link)

- Consumi energetici estremamente ridotti

Limitazioni:

- Rischio di interferenze nella banda 2.4 GHz
- Complessità nella gestione di reti molto estese
- Frammentazione tra profili e versioni differenti
- Velocità non adatta a trasferimenti di dati intensivi

Philips Hue, ad esempio, utilizza Zigbee per controllare fino a 50 lampadine con un singolo bridge, offrendo sincronizzazione precisa e latenza impercettibile.

5.3.2 Z-Wave: l'alternativa su frequenze dedicate

Z-Wave si distingue per l'utilizzo di frequenze sub-GHz (868 MHz in Europa, 908 MHz negli USA), che garantiscono una maggiore penetrazione attraverso muri e ridotte interferenze rispetto alla banda 2.4 GHz.

Caratteristiche distintive:

- Interoperabilità certificata tra dispositivi Z-Wave
- Portata estesa fino a 100 metri in campo aperto
- Topologia mesh con routing source-routed ottimizzato
- Limite di 232 nodi per rete, sufficiente per l'ambito residenziale

La sua velocità massima, pari a 100 kbps, lo rende inadatto a carichi di dati elevati, ma perfetto per sistemi di controllo. Un impianto di sicurezza domestica può includere sensori di movimento, contatti magnetici per porte/finestre e sirene ad alta affidabilità.

5.3.3 Wi-Fi: potenza e versatilità

Il Wi-Fi domina per capacità di banda e diffusione. La presenza capillare di router domestici riduce la necessità di infrastrutture dedicate, rendendolo ideale per dispositivi che richiedono elevato throughput.

Vantaggi competitivi:

- Larghezza di banda elevatissima, adatta a video e trasferimenti intensivi
- Infrastruttura già presente nella maggior parte delle abitazioni
- Supporto IP nativo, ideale per integrazione cloud
- Ottimizzazioni recenti in Wi-Fi 6 per dispositivi IoT (es. Target Wake Time)

Sfide operative:

- Consumo energetico elevato, inadatto a dispositivi a batteria
- Degrado prestazionale con molti dispositivi connessi a un singolo access point

- Latenza variabile in presenza di congestione di rete
- Hardware più costoso rispetto ad alternative low-power

Le videocamere IP rappresentano un'applicazione ideale: richiedono banda elevata e sono alimentate da rete elettrica, eliminando il vincolo energetico W.-F. Alliance 2021.

5.3.4 Thread: l'evoluzione IP-native

Thread è un protocollo mesh moderno progettato per supportare IPv6 nativamente, con un'architettura leggera e sicura adatta all'era dell'interoperabilità e del cloud.

Innovazioni chiave:

- Supporto IPv6 nativo con instradamento end-to-end
- Sicurezza avanzata con crittografia AES e gestione automatica delle chiavi
- Commissioning semplice via smartphone
- Mesh self-healing con tempi di riconvergenza rapidi

Le sue latenze sono paragonabili a Zigbee (20–50 ms), ma con un'architettura più moderna e scalabile. Dispositivi come Apple HomePod mini o Google Nest Hub fungono da border router per reti Thread, facilitando l'adozione senza componenti aggiuntivi Group 2023.

5.3.5 Matter: l'unificatore dell'ecosistema

Matter si propone come livello applicativo universale, operando sopra protocolli esistenti come Thread, Wi-Fi ed Ethernet. Il suo obiettivo è garantire interoperabilità trasparente tra piattaforme e produttori.

Punti di forza:

- Compatibilità trasversale tra Apple, Google, Amazon, Samsung
- Sicurezza integrata nel design, con certificazione obbligatoria
- Commissioning tramite QR code o NFC
- Comunicazione locale senza necessità di cloud

Matter introduce un overhead minimo (circa 5–10% di latenza aggiuntiva), ma il vantaggio in termini di compatibilità compensa ampiamente. Un termostato compatibile può essere gestito indistintamente da Siri, Google Assistant o Alexa, mantenendo la stessa qualità d'interazione C. S. Alliance 2023.

Parametro	Zigbee	Z-Wave	Wi-Fi	Thread	Matter
Banda	2.4 GHz	Sub-GHz	2.4/5 GHz	2.4 GHz	-
Topologia	Mesh	Mesh	Point-to-point	Mesh	-
Velocità max	250 kbps	100 kbps	>100 Mbps	250 kbps	-
Energia	Molto bassa	Bassa	Alta	Bassa	Variabile
Interoperabilità	Limitata	Alta (cert.)	Variabile	Alta	Massima

Tabella 5.2: Confronto sintetico tra protocolli e standard IoT in ambito domotico

5.4 Scalabilità dei protocolli in ambienti domestici complessi

Man mano che le abitazioni intelligenti si arricchiscono di sensori, attuatori e dispositivi di controllo, il tema della **scalabilità** diventa centrale. Un sistema domotico moderno non si limita più ad accendere qualche luce o a regolare il termostato: può arrivare a gestire centinaia di elementi distribuiti in ambienti ampi e strutturati. In questo contesto, è fondamentale comprendere come i principali protocolli IoT reagiscano all'aumento della complessità della rete.

5.4.1 Scalabilità per protocollo

5.4.1.1 Zigbee: tra teoria e realtà

Zigbee dichiara il supporto fino a 65.000 dispositivi per rete, un numero che, sulla carta, garantirebbe ampie possibilità di espansione. Tuttavia, in ambito residenziale, questa soglia è ben lontana dalla realtà operativa.

Già superata la soglia dei 200-300 dispositivi, cominciano a emergere difficoltà pratiche:

- Latenze maggiori dovute al routing tra nodi multipli
- Congestione nella banda a 2.4 GHz, soprattutto in ambienti densi
- Rallentamenti durante aggiornamenti firmware distribuiti
- Complessità crescente nella configurazione e manutenzione

Una strategia spesso adottata è la creazione di **sotto-reti logiche** distinte, ciascuna gestita da un coordinator dedicato, per esempio separando l'illuminazione dalla climatizzazione o dai sistemi di sicurezza.

5.4.1.2 Z-Wave: solido entro i propri limiti

Z-Wave ha un limite teorico molto più contenuto: 232 dispositivi per rete. Tuttavia, per la maggior parte delle abitazioni — anche quelle di grandi dimensioni — si tratta di un numero più che sufficiente. La gestione più semplice e il minor rischio di congestione radio, grazie all'uso della banda sub-GHz, lo rendono una scelta solida e prevedibile.

Un'abitazione con circa 100 dispositivi (tra interruttori, sensori e attuatori) rientra tranquillamente nei limiti del protocollo, offrendo ancora margine per ulteriori espansioni.

5.4.1.3 Thread e Matter: progettati per crescere

Thread è stato pensato fin dall'inizio per reti scalabili, affidabili e facilmente gestibili:

- I router mesh distribuiti bilanciano il traffico in modo dinamico
- L'uso nativo di IPv6 semplifica il routing e la gestione
- La rete si auto-configura e auto-ripara in caso di guasti

Test su installazioni reali mostrano che anche con oltre 200 dispositivi, i tempi di risposta restano sotto i 100 ms nel 95° percentile, con una degradazione molto graduale delle prestazioni all'aumentare del carico.

Matter, appoggiandosi a Thread (e in parte al Wi-Fi), eredita e potenzia questa capacità, offrendo al tempo stesso interoperabilità tra ecosistemi e gestione centralizzata semplificata.

5.4.2 Strategie di progettazione per reti complesse

5.4.2.1 Progettare la rete per livelli

Quando i dispositivi aumentano, progettare in modo gerarchico diventa essenziale. Una buona architettura divide la rete in tre livelli logici:

1. **Livello Edge**: i dispositivi periferici (sensori, attuatori) che eseguono compiti specifici
2. **Livello di Aggregazione**: hub locali o controller di zona che raccolgono e instradano i dati
3. **Livello Core**: un controller principale (o cloud gateway) che integra, elabora e coordina tutto il sistema

Questa suddivisione migliora la stabilità, semplifica la manutenzione e consente di isolare eventuali malfunzionamenti, evitando che si propaghino all'intero sistema.

5.4.2.2 Separare per funzione: la rete è più leggibile

Un'altra strategia efficace è la suddivisione dei dispositivi in reti logiche in base alla loro funzione:

- **Rete Sicurezza**: dispositivi critici come sensori di movimento, allarmi e serrature (dove l'affidabilità è prioritaria)
- **Rete Comfort**: luci, termostati e tapparelle (ottimizzati per reattività e basso consumo)
- **Rete Media**: smart TV, speaker, videocamere (dove la banda e la connessione stabile sono fondamentali)

In questo modo si ottimizzano i protocolli per ciascun gruppo: Z-Wave può essere usato per la sicurezza, Zigbee o Thread per l'illuminazione, e il Wi-Fi per streaming e intrattenimento.

5.4.3 Conclusioni sulla scalabilità

In sostanza quando ci troviamo a realizzazione di sistemi domotici complessi, la prima vera sfida è quella della scalabilità che non si esaurisce nei soli numeri dichiarati dai produttori. Al contrario, deve essere fondamentale che la rete sia in grado di mantenere buoni tempi di risposta, sia semplice nella gestione ed affidabilità, sopratutto quando il numero di dispositivi collegati aumenta sensibilmente.

Ogni protocollo che abbiamo visto finoea presenta caratteristiche diverse in questo scenario.
Zigbee può scalare bene, ma richiede una buona esperienza nella progettazione di rete per evitare colli di bottiglia.
Z-Wave, per la sua semplicità di configurazione e la sua stabilità, ottenuta sfruttando le banda sub-GHz con meno traffico, si adatta perfettamente a contesti residenziali di dimensioni medio-piccole.
Thread e Matter, diversamente dai precedenti, offrono un approccio più moderno e flessibile, risultando particolarmente indicati per installazioni più grandi, complesse e in continua evoluzione, spinto anche dall'innovazione che le proncipali aziende stanno dando a questo protocollo.

In conclusione, per definire il successo di una rete domotica complessa e grande, non bisogna guardare solo dal protocollo che abbiamo scelto, ma soprattutto da come viene disegnata: una buona progettazione, cola presenza di segmentazioni funzionali, la definizione di una organizzazione gerarchica, consentono di ottenere risultati affidabili e duraturi, qualunque sia la tecnologia utilizzata.

Capitolo 6

Prospettive Future nella Domotica Residenziale

6.1 Introduzione

Dopo aver esaminato nel Capitolo 5 le prestazioni, l'affidabilità e la scalabilità dei principali protocolli di comunicazione impiegati nelle abitazioni intelligenti, ora andiamo ad esplorare le tecologie emergenti per le smart home.

Negli ultimi anni, la casa ha smesso di essere solo il nostro spazio abitato, ma si sta trasformando progressivamente in un ecosistema interattivo. Questo cambiamento segue una trasformazione culturale e tecnologica più ampia, che rispecchia ilnostro modo di vivere, oramai siamo abituati a lavoriamo e interagiamo con l'ambiente che ci circonda. La domotica quindinon è più appannaggio di pochi appassionati o early adopter ma è diventata una componente concreta dell'abitare contemporaneo.

Questa evoluzione tuttavia non è lineare né priva di ostacoli. L'interoperabilità tra dispositivi, la protezione dei dati personali, l'efficienza energetica e l'inclusività sono sfide reali. Ma sono anche i punti su cui costruire una nuova idea di casa.

Dopo anni in cui i vari produttori fornivano soluzioni frammentate e proprietarie, oggi una nuova visione orientata sta guidando gli sviluppi concentrandosi su interoperabilità, sostenibilità e intelligenza diffusa. Questa transizione non riguarda soltanto l'arrivo di nuovi dispositivi e nuove tecnologie, ma è un cambiamento più profondo, la casa interagisce con i suoi abitanti impara da loro e si adatta in modo intelligente.

Le abitazioni del futuro saranno ambienti realmente smart, capaci di prevedere i nostri bisogni, reagire in tempo reale, proteggere dati sensibili e garantire accessibilità a tutti. In questo capitolo analizziamo le nuove tendenze emergenti, valutandone potenzialità e sfide.

6.2 Lo standard Matter e i protocolli IP-native

6.2.1 Matter: interoperabilità come fondamento

Matter non è soltanto un nuovo standard, ma è il simbolo di una storica alleanza tra le principali case produttrici dell'industria tecnologica quali Apple, Google, Amazon,

Samsung, per superare i limiti della frammentazione e della interoperatività. Nasce come evoluzione del progetto CHIP (Connected Home over IP), con l'obiettivo di rendere compatibili tra loro dispositivi di diversi produttori.

Il punto di forza di Matter è basato su un modello applicativo standardizzato, che rende possibile un dialogo strutturato e uniforme tra tutti i componenti della rete domestica. La configurazione di nuovi dispositivi avviene in modo semplice e tramite dei wizard attivabili tramite QR code o NFC, supporta inolte il controllo multi-ecosistema, questo rende possibile l'utilizzo dello stesso dispositivo con più assistenti vocali o app differenti, senza conflitti, ad esmpio in casa posso controllare una luce sia da Siri che da Alexa. Inoltre, Matter supporta e privilegia il controllo locale, riuscendo così a garantire continuità anche in assenza di connessione Internet.

Basato sul protocollo di rete IPv6 e protetto dallo standard di crittografia TLS 1.3, Matter combina la scalabilità con la sicurezza.

6.2.2 Thread: architettura distribuita e resiliente

Il protocollo Thread, spesso utilizzato in abbinamento con Matter, è un protocollo basato su rete mesh IP-native, progettato specificatamente per l'utilizzo in ambiente IoT. Tra le sue caratteristiche principali, ogni nodo ha un indirizzo IP univoco, la rete si autoconfigura e si auto-ripara, senza necessità di un coordinatore centrale. In caso di guasto del'Hub centrale leader, un nuovo leader viene eletto automaticamente, garantendo affidabilità e continuità.

Thread, come già analizzato per la sua architettura mesh e sicurezza nativa, si afferma ad oggi come la componente centrale per le reti domestiche, in grado di garantire resilienza ed estendibilità, soprattutto in abbinamento allo standard Matter

L'integrazione di Thread in dispositivi come Apple HomePod, Alexa e Google Home ne facilitano l'adozione domestica, senza bisogno di doversi munire di Hub dedicati.

6.3 Tecnologie emergenti per la casa intelligente

6.3.1 Intelligenza artificiale nella vita domestica

L'adozione dell'intelligenza artificiale sta trasformando l'esperienza abitativa da una serie di automatismi e scenari che apprendono, anticipano e si adattano al nostro stile di vita.

Esempio evolutivo: oggi noi quando rientriamo in casa, diciamo "Alexa, accendi la luce"; un domani non tanto lontano, la casa riconoscerà il nostro rientro, rileverà la scarsa luminosità e accenderà automaticamente la luce più adatta, predisponendo l'ambiente secondo le nostre abitudini.

L'adozione del *machine learning on-device* permette l'elaborazione dei dati direttamente sul dispositivo, riducendo la dipendenza dal cloud e la trasmissione di dati. Questo porta benefici concreti come una minore latenza, una maggiore privacy ed una personalizzazione maggiore.

6.3.1.1 Apprendimento federato

Attraverso il *federated learning*, i dispositivi intelligenti elaboreranno i dati localmente e comunicheranno solo gli aggiornamenti del modello, così garantiranno che nessuna informazione sensibile verrà mai trasferita o memorizzata nel cloud.

6.3.2 Reti mesh e Wi-Fi di nuova generazione

Dopo aver evidenziato i benefici di una rete mesh nel capitolo precedente, le reti mesh oggi evolvono con l'integrazione dei nuovi standard Wi-Fi e Thread, abilitando così scenari più reattivi e modulari.

Wi-Fi 6, 6E e 7 rappresentano tappe fondamentali nell'evoluzione delle reti:

- **Wi-Fi 6**: introduce OFDMA, TWT e BSS Coloring, aumentando efficienza e riducendo la latenza.
- **Wi-Fi 6E**: aggiunge la banda a 6 GHz, liberando nuovi canali per dispositivi smart.
- **Wi-Fi 7**: promette latenze ultra-basse e velocità fino a 46 Gbps.

Una breve tabella riassuntiva può essere utile nel capitolo:

Versione	Anno	Banda	Caratteristiche principali
Wi-Fi 5	2014	2.4 / 5 GHz	Alta velocità, no ottimizzazioni IoT
Wi-Fi 6	2019	2.4 / 5 GHz	OFDMA, TWT, efficienza migliorata
Wi-Fi 6E	2020	6 GHz	Nuovi canali, meno interferenze
Wi-Fi 7	2024	2.4 / 5 / 6 GHz	MLO, latenza bassa, throughput massimo

Tabella 6.1: Evoluzione dello standard Wi-Fi per ambienti smart home

6.3.3 Edge e fog computing domestico

L'elaborazione locale dei dati tramite fog computing consente:

- Risposte in tempo reale
- Resilienza in caso di assenza di Internet
- Protezione dei dati sensibili
- Riduzione del traffico e costi cloud

Progetti come K3s, una distribuzione leggera e semplificata di Kubernetes, pensata per ambienti IoT permetteranno l'orchestrazione di microservizi direttamente sugli hub domestici, trasformando così ogni stanza in un nodo intelligente.

6.4 Privacy, sicurezza e fiducia digitale

6.4.1 Le nuove sfide dell'abitazione intelligente

Sebbene l'intelligenza artificiale migliori l'automazione e l'efficienza dele nostre case, essa richiede un accesso costante ai nostri dati sensibili come le nostre abitudini quotidiane, i pattern di presenza nella casa e le nostre preferenze personali. Questa dipendenza impone l'adozione di diverse rigorose misure di sicurezza e un approccio responsabile al trattamento dei dati.

6.4.2 Strategie di protezione

- **Zero Trust Architecture**: ogni richiesta è validata, anche all'interno della rete.
- **Segmentazione delle reti**: per limitare i danni in caso di compromissione.
- **Crittografia omomorfica**: elabora dati cifrati senza decifrarli.
- **Blockchain per audit trail**: tracciabilità sicura delle azioni eseguite.

6.5 Inclusività come principi guida

6.5.1 Tecnologia accessibile a tutti

Domotica inclusiva significa:

- Interfacce adattive per anziani e disabili
- Supporto vocale, gestuale e aptico
- Soluzioni retrofit per abitazioni esistenti
- Promozione dell'open source e del fai-da-te

6.6 Conclusioni: la casa come alleata

Non si tratta più solo di rendere la casa "smart", ma di saper costruire un ambiente che sia in grado di ascoltare, apprendere e rispondere in modo etico e personalizzato. Il futuro della domotica non si misura dal numero di dispositivi installati in una casa, ma dalla loro capacità di adattarsi all'ambiente domestico in cui sono inseriti, di rispettare e migliorare la vita dei suoi abitanti.

Capitolo 7

Gestione di Dispositivi Multimarca

7.1 Introduzione

Il Capitolo precedente ha evidenziato come le prospettive future della domotica residenziale si stiano progressivamente orientando verso modelli sempre più aperti, interoperabili e intelligenti. Tuttavia, affinché queste promesse si traducano in un'esperienza concreta per l'utente finale, è necessario affrontare una delle sfide più complesse del settore: la gestione di dispositivi di marche e protocolli diversi all'interno di un unico ambiente domestico.

Immagina di essere in un negozio di elettronica. Vuoi rendere la tua casa più smart e finalmente ti decidi: una bella lampadina connessa, magari Philips. Poi noti un termostato intelligente, quello della Nest ti convince. La serratura smart più sicura? Yale. E già che ci sei, aggiungi anche un paio di telecamere Arlo, che sembrano avere ottime recensioni.

Torni a casa soddisfatto, pronto a configurare tutto. Ma in pochi minuti la sensazione cambia: ogni dispositivo richiede la sua app, il suo account, il suo hub. Le lampadine non parlano con il termostato, la serratura ignora le telecamere, e tu inizi a sentire che più che in una casa intelligente, ti trovi in una casa... **complicata**. È come se ogni dispositivo parlasse una lingua diversa, e l'utente dovesse improvvisarsi traduttore simultaneo, passando da un'app all'altra con crescente frustrazione.

Ecco il paradosso della domotica moderna: più scelta abbiamo, più difficile diventa mettere tutto insieme. Questo capitolo entra nel cuore di questa sfida. Perché far dialogare dispositivi di marche diverse non è solo un problema tecnico: significa garantire coerenza nell'esperienza d'uso, mantenere sicurezza e affidabilità, e soprattutto non perdere la testa ogni volta che si aggiunge qualcosa di nuovo.

7.2 La sfida dell'interoperabilità

7.2.1 Le radici del problema

Quando pensiamo all'interoperabilità nella domotica, potremmo immaginarla come un semplice problema tecnico da risolvere. Ma la realtà è molto più complessa. Questa frammentazione nasce da anni — anzi, decenni — di scelte industriali fatte non tanto per facilitare la vita degli utenti, quanto per rafforzare la posizione di mercato dei produttori. Ogni azienda ha costruito il proprio ecosistema come un "giardino recintato", dove tutto funziona bene finché resti dentro, ma diventa complicato appena provi a integrare qualcosa di diverso.

7.2.1.1 La Torre di Babele dei protocolli

La situazione attuale assomiglia a una moderna Torre di Babele: ogni produttore parla la propria lingua, rendendo difficile – se non impossibile – far comunicare dispositivi diversi tra loro.

- **Protocolli proprietari**: Ogni grande azienda ha sviluppato il proprio "dialetto". Lutron usa ClearConnect, Insteon ha un protocollo dual-band tutto suo, Somfy parla RTS o io-homecontrol. Il risultato? Dispositivi eccellenti, ma incapaci di capirsi tra loro.
- **Varianti su uno stesso tema**: Anche quando si sceglie lo stesso linguaggio di base, come Zigbee, non è detto che ci sia comprensione. Philips Hue adotta Zigbee Light Link, altri preferiscono Zigbee Home Automation: stessi fondamentali, ma grammatica e accento differenti, che spesso non si comprendono.
- **Livelli diversi di astrazione**: Alcuni protocolli lavorano "sotto il cofano", a livello fisico (come Z-Wave), altri agiscono più in superficie, a livello di esperienza utente e applicazioni (come HomeKit). Tradurre da uno all'altro è come passare da codice macchina a conversazione naturale: servono interpreti intelligenti.
- **Sicurezza che non si parla**: Anche i modelli di sicurezza variano. Diverse tecniche di crittografia e autenticazione rendono difficile, e talvolta rischioso, mettere in comunicazione dispositivi di produttori diversi senza compromettere la protezione dei dati.

7.2.1.2 L'impatto sull'utente finale

La frammentazione dell'ecosistema domotico si traduce, per l'utente finale, in un'esperienza spesso frustrante e tutt'altro che "smart":

Troppe app, poca chiarezza: Secondo una ricerca del 2023, l'utente medio di una casa intelligente utilizza tra le 8 e le 12 app diverse per controllare i propri dispositivi. Ogni produttore ha la sua, ognuna con interfaccia diversa, logiche diverse, notifiche diverse. Il risultato? Il telefono diventa un campo di battaglia digitale, e avere una visione d'insieme del sistema è praticamente impossibile.

Automazioni che faticano a cooperare: Una semplice regola, come "quando esco di casa, spegni tutte le luci e abbassa il termostato", può trasformarsi in un puzzle complicato. Ogni pezzo della catena – lampadine, riscaldamento, sensori di presenza – parla una lingua diversa, e spesso non si capiscono. Una parte funziona, l'altra no. E l'utente si ritrova a dover intervenire manualmente.

Lentezza imprevista: Ogni volta che un comando deve attraversare più livelli – ad esempio da un hub Zigbee, a un bridge proprietario, poi al cloud del produttore, da lì a un altro servizio cloud, e infine al dispositivo – si accumulano ritardi. Quello che dovrebbe essere un'azione immediata può richiedere diversi secondi. Non è solo fastidioso, ma anche poco affidabile.

Costi invisibili, ma reali: Oltre al prezzo dei dispositivi, spesso bisogna acquistare hub aggiuntivi, bridge, gateway, e magari anche sottoscrivere abbonamenti per funzionalità cloud avanzate. Una casa "veramente smart" può arrivare a richiedere 3, 4 o 5 hub diversi per funzionare come si desidera.

7.2.2 L'evoluzione verso standard comuni

Per anni, la domotica ha viaggiato su binari paralleli, con ogni produttore convinto di poter costruire un ecosistema chiuso e autosufficiente. Tuttavia, col tempo è diventato evidente che questa frammentazione non giova a nessuno: complica la vita agli utenti, rallenta l'adozione di massa e genera una percezione di tecnologia "instabile" o poco matura. Quando persino i tecnici iniziano a faticare per far dialogare tra loro i dispositivi, è chiaro che serve un cambio di paradigma.

Per fortuna, una parte sempre più ampia del settore ha riconosciuto che l'interoperabilità non è solo un vantaggio competitivo, ma una necessità. E così è iniziata un'evoluzione importante, guidata da due forze complementari: da un lato la spinta delle comunità open source, dall'altro la convergenza delle grandi aziende su standard comuni.

7.2.2.1 Il movimento open source

Nel vuoto lasciato da un'industria ancora troppo frammentata, la community open source ha saputo costruire soluzioni concrete, flessibili e sorprendentemente avanzate. Sviluppatori indipendenti, appassionati, maker e professionisti IT si sono uniti per creare piattaforme capaci di integrare decine – se non centinaia – di dispositivi diversi, superando le barriere imposte dai vendor.

Ecco alcune delle iniziative più significative:

- **Home Assistant**: Nato nel 2013 come progetto personale di Paulus Schoutsen, è diventato oggi il punto di riferimento per l'integrazione multimarca. Con oltre 2000 integrazioni supportate, permette di unificare luci, termostati, sensori, elettrodomestici e molto altro in un'unica interfaccia Home Assistant 2024.

- **OpenHAB**: Un altro gigante del mondo open source, pensato fin dall'inizio con un'architettura modulare orientata alla flessibilità. Permette di scrivere logiche complesse in linguaggi come JavaScript, Groovy o Python, rendendolo ideale per chi ha esigenze articolate *openHAB - empowering the smart home* 2023.

- **Node-RED**: Una piattaforma di programmazione visuale che ha conquistato il cuore di molti utenti tecnici. Permette di creare automazioni collegando nodi con un semplice drag-and-drop, visualizzando in tempo reale il flusso dei dati. È spesso utilizzata in combinazione con Home Assistant per estendere ulteriormente le capacità *Node-RED - Flow-based programming for the Internet of Things* 2024.

7.2.2.2 L'alleanza dell'industria: Matter

Nel mondo dell'elettronica di consumo, vedere Apple, Google, Amazon e Samsung seduti allo stesso tavolo non è solo raro: è quasi impensabile. Eppure è successo. Dopo anni di ecosistemi chiusi, incompatibilità frustranti e guerre silenziose per il controllo della casa connessa, le grandi aziende hanno riconosciuto che la vera innovazione non passa (più) dall'esclusione, ma dalla collaborazione.

Da questo storico compromesso è nato **Matter**, uno standard aperto che ambisce a diventare il "linguaggio comune" della domotica. Non si tratta semplicemente di un nuovo protocollo, ma di un vero cambio di paradigma: finalmente i dispositivi possono parlarsi senza traduttori, senza ponti complicati, e senza la necessità di scegliere da subito "da che parte stare".

Il percorso per arrivare a Matter non è stato breve né semplice:

- **2019**: Nasce *Project CHIP* (Connected Home over IP), inizialmente come iniziativa tecnica congiunta per risolvere i problemi di compatibilità più evidenti.
- **2021**: Il progetto cambia nome in *Matter* e vengono pubblicate le prime specifiche ufficiali.
- **2022**: I primi dispositivi certificati fanno la loro comparsa sul mercato, seguiti da aggiornamenti firmware che permettono anche a dispositivi esistenti di essere compatibili.
- **2023-2024**: L'adozione cresce rapidamente, con il supporto esteso in tutti i principali ecosistemi e una base di dispositivi sempre più ampia.

Ciò che rende Matter davvero rivoluzionario è l'approccio mentalmente inclusivo. Invece di obbligare l'utente a scegliere tra HomeKit, Google Home o Alexa, Matter consente che uno stesso dispositivo venga controllato da più piattaforme contemporaneamente. Una lampadina smart può essere aggiunta sia all'iPhone che all'altoparlante Google, e rispondere a entrambi. Non è più l'utente a doversi adattare al sistema, ma il contrario.

Ma c'è anche un risvolto strategico: il successo di Matter non è solo un favore fatto agli utenti, ma anche un riconoscimento, da parte dei big tech, che la casa connessa non può più essere una somma di silos isolati. Serve coerenza, semplicità, trasparenza.

Matter segna, quindi, un passaggio da un'epoca di lock-in tecnologici a un'era di collaborazione e apertura. Una scelta coraggiosa, ma necessaria, per fare della domotica non un lusso per esperti, ma una realtà accessibile a tutti.

Appendice A

Glossario dei termini e degli acronimi

IoT Insieme di dispositivi e sensori collegati a Internet, capaci di comunicare autonomamente e rendere intelligenti ambienti e oggetti quotidiani.

BLE Bluetooth Low Energy — Standard wireless a basso consumo energetico.

Zigbee Protocollo wireless basato su IEEE 802.15.4, ottimizzato per reti mesh a corto raggio.

Z-Wave Protocollo wireless a bassa potenza, usato per applicazioni di domotica.

Wi-Fi Wireless Fidelity — Tecnologia di rete locale senza fili basata su IEEE 802.11.

Thread Protocollo di rete IPv6-based pensato per dispositivi IoT.

Matter Standard aperto per l'interoperabilità tra dispositivi smart, sviluppato dalla CSA.

HomeKit Piattaforma sviluppata da Apple per controllare e gestire in maniera semplice e sicura i dispositivi domestici intelligenti tramite dispositivi iOS.

Gateway Dispositivo che consente la comunicazione tra reti o protocolli differenti.

API Application Programming Interface — Interfaccia che permette l'interazione tra software.

Hub Dispositivo che agisce da centro di controllo, permettendo a diversi dispositivi smart di comunicare tra loro e con l'utente.

KNX Standard aperto per l'automazione degli edifici, utilizzato principalmente in sistemi cablati per applicazioni domotiche.

Rete mesh Tipologia di rete in cui ciascun dispositivo è collegato direttamente a più altri, aumentando l'affidabilità e l'efficienza nella comunicazione.

IPv6 Versione più recente del protocollo Internet, che consente un numero quasi illimitato di indirizzi IP.

Hub centrale Dispositivo centrale che coordina e gestisce le comunicazioni tra dispositivi intelligenti in una rete domotica.

RS-485 Standard di comunicazione seriale cablato, resistente alle interferenze e utilizzato principalmente in ambienti industriali e domotici per connessioni su lunghe distanze.

VLAN Rete virtuale che separa logicamente gruppi di dispositivi all'interno della stessa rete fisica, migliorando sicurezza e gestione.

IDS Sistema che monitora il traffico di rete per identificare e segnalare eventuali intrusioni o attività sospette non autorizzate.

Firmware Software fondamentale, installato permanentemente sui dispositivi hardware per controllare direttamente le loro operazioni di base.

DTLS Datagram Transport Layer Security — Protocollo di sicurezza che fornisce comunicazioni cifrate per dispositivi con risorse limitate, basato su UDP.

VLAN Rete virtuale che separa logicamente gruppi di dispositivi all'interno della stessa rete fisica, migliorando sicurezza e gestione.

IDS Sistema che monitora il traffico di rete per identificare e segnalare eventuali intrusioni o attività sospette non autorizzate.

Firmware Software fondamentale, installato permanentemente sui dispositivi hardware per controllare direttamente le loro operazioni di base.

DTLS Datagram Transport Layer Security — Protocollo di sicurezza che fornisce comunicazioni cifrate per dispositivi con risorse limitate, basato su UDP.

Tag Dispositivo utilizzato per attivare automazioni domotiche. Può essere passivo (NFC/RFID, senza batteria, funziona al tocco) o attivo (BLE/beacon, con batteria, rileva la presenza a distanza).

MFA Multi-Factor Authentication – Metodo di autenticazione che richiede all'utente di fornire due o più prove ("fattori") per verificare la propria identità prima di concedere l'accesso a un sistema o servizio

Appendice B

Appendice Tecnica: Configurazione di un sistema HomeKit

Esempio di configurazione YAML per Homebridge

```
{
  "bridge": {
    "name": "Homebridge",
    "username": "CC:22:3D:E3:CE:30",
    "port": 51826,
    "pin": "031-45-154"
  },
  "description": "Configurazione base per accessori BTicino e Netatmo",
  "accessories": [],
  "platforms": [
    {
      "platform": "netatmo",
      "name": "Netatmo Platform",
      "client_id": "TUO_CLIENT_ID",
      "client_secret": "TUO_CLIENT_SECRET",
      "username": "email@example.com",
      "password": "password"
    }
  ]
}
```

Schermata di esempio

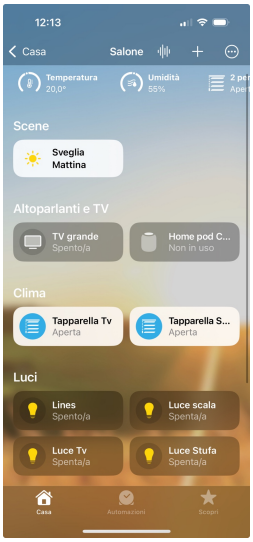

Figura B.1: Interfaccia Apple Home con dispositivi configurati

Bibliografia

Alliance, Connectivity Standards (2023). *Matter Overview White Paper*. Accessed: 2025-08-05. URL: https://csa-iot.org/wp-content/uploads/2022/03/Matter_Security_and_Privacy_WP_March-2022.pdf.

— (2024). *Zigbee Specification*. Accessed: 2025-08-05. URL: https://csa-iot.org/developer-resources/zigbee/.

Alliance, Wi-Fi (2021). *Wi-Fi and the Internet of Things*. Accessed: 2025-08-05. URL: https://www.wi-fi.org/internet-things-iot.

— (2022). *Wi-Fi CERTIFIED 6 Technology Overview*. Accessed: 2025-08-05. URL: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6.

Alliance, Z-Wave (2023). *Z-Wave Specification*. Accessed: 2025-08-05. URL: https://z-wavealliance.org/technology-overview/.

Antonakakis, M., T. April e M. et al. Bailey (2017). *Understanding the Mirai Botnet*. URL: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

Group, Thread (2023). *Thread Technical Overview*. Accessed: 2025-08-05. URL: https://www.threadgroup.org/What-is-Thread/Overview.

Home Assistant (2024). *Documentation and Integrations*. Accesso il 10 aprile 2025. URL: https://www.home-assistant.io/.

Node-RED - Flow-based programming for the Internet of Things (2024). Accessed: 2025-08-07. URL: https://nodered.org.

openHAB - empowering the smart home (2023). Accessed: 2025-08-07. URL: https://www.openhab.org.

Wikipedia contributors (2024). *Domotica*. Accesso il 10 aprile 2025. URL: https://it.wikipedia.org/wiki/Domotica.