APPUNTI
SISTEMI
PER L'IOT

Insegnamento di Sistemi per l'IOT tenuto dal Prof. Luca Romanelli

stilato da

Stefano Zizzi, Luis Frasheri

Basato sugli appunti di

Emanuele Grasso

Università degli Studi di Urbino
Informatica Applicata

GENNAIO 2024

Indice

Parte I

Introduzione

Capitolo 1

Fondamenti dei Sistemi per l'Internet delle Cose

1.1 Definizioni

Per il prossimo futuro si stima una crescita del 20% annuo sul numero dei dispositivi connessi. Requisiti minimi affinché un dispositivo possa dirsi parte di IoT:

- Deve avere capacità computazionali;
- Deve avere lo stack minimo dei protocolli per consentire una comunicazione efficace attraverso internet (non deve essere per forza connesso ad internet);
- Non deve essere una periferica storicamente connessa ad internet.

Tra i dispositivi vanno inclusi i dispositivi perimetrali detti *Edge Devices*, che sono apparecchi progettati per operare in condizioni poco ottimali, quindi tempo atmosferico avverso oppure fornitura di energia non costante. Generalmente sono nodi gestiti che vanno posizionati vicino alla fonte del dato e funzionano in modalità Hub-and-Spoke con un *Edge Computer*.

Modello Hub-and-Spoke Modello che si basa su un hub centralizzato che "facilita" le operazioni dei sistemi periferici; è un modello generale che non riguarda unicamente i sistemi elettronici. In ambito IoT, molti dispositivi non hanno capacità di connessione e vengono quindi utilizzati all'interno di questo modello dove il ruolo dell'hub lo assume un piccolo elaboratore chiamato edge computer.

Industial IoT (IIoT) Segmento che cresce con maggiore velocità e diffusione, tradizionalmente indicato con Operational Technology (OT), riguarda il monitoraggio ed il controllo di hardware e software in tempo reale. Si basa su computer e server in sede ed il sistema hardware e software è indicato con l'acronimo Supervisory Control And Data Acquisition (SCADA).
Differenze tra Operational Technology (OT) e Information Technology (IT):

- *Operational Technology (OT)*: sensoristica, tempo di esercizio lungo, sicurezza del sistema;
- *Information Technology (IT):* distribuzione dei dati, workgroup, sicurezza dei dati.

Inoltre, il vincolo del *tempo reale*[1], così come il tempo di esercizio e la sicurezza, sono caratteristiche peculiari dei sistemi industriali, prediligendo l'affidabilità alla velocità.

1.2 Casi d'Uso

I casi d'uso sono innumerevoli, per citarne alcuni:

- **Ambito consumer**: Primo segmento ad adottare dispositivi connessi ad internet a diretto contatto con le persone. La difficoltà più grande consiste nel proliferarsi degli standard, poiché esistono più protocolli per realizzare una WPAN, tutti non inoperabili, a meno di appositi gateway.

[1] Tempo reale: privo di ritardi eccessivi.

- **Ambito healthcare**: Compete con l'industria manufatturiera e la logistica per il miglior Return Of Investment (ROI). Monitoraggio veloce e flessibile di pazienti, ovunque si trovino.
  I vincoli per la realizzazione di dispositivi sono molto stringenti e necessitano di:
  - Approvazione da parte di enti regolatori;
  - Gestire la sicurezza dei dati considerati "sensibili";
  - Essere realizzati con standard di qualità pari a quella dei sistemi ospedalieri;
  - Poter comunicare con i centri di monitoraggio ininterrottamente;
  - Potersi connettere alla rete ospedaliera.
- **Ambito logistica**: Attualmente un veicolo è dotato, mediamente, di 100 sensori (numero che sta per raddoppiare), aumentando drasticamente su veicoli a rotaia o navali.
- **Ambito agricoltura e ambiente**: Per la salute del bestiame, analisi del suolo, uso efficiente dell'acqua, predizione di condizioni climatiche o geologiche pericolose.
- **Ambito energia**: Monitoraggio della produzione e dei consumi di energia in tempo reale. Molti siti di produzione di energia sono collocati in ambienti "ostili".
- **Ambito Smart City**: Insieme di infrastrutture, cittadini e veicoli interconnessi inmaniera intelligente. Ottimo rapporto costi/benefici, ma con necessità di plasmare e dimensionare la rete in maniera altrettanto intelligente.

Capitolo 2

Architettura Generale di un Sistema IoT

2.1 Architettura di un Sistema IoT

Il sistema IoT parte da sensori remoti che traducono effetti fisici analogici in segnali digitali, trasmettendoli fino a raggiungere un data center. Il campionamento è il primo passo del processo di conversione analogico-digitale e consiste in:

1. Prelievo di campioni (uno ogni Δt di tempo)[1] da un segnale analogico e continuo nel tempo;
2. Il risultato è un segnale analogico in tempo discreto che viene quantizzato, codificato e reso accessibile a qualsiasi elaboratore.

Teorema di Nyquist-Shannon: Dato un segnale analogico $s(t)$ la cui banda di frequenze è limitata dalla frequenza fM; Dato un $n \in Z$, allora,il segnale può essere ricostruito a partire dai suoi campioni $s(n\Delta t)$ presi a frequenza $f_S = 1\ \Delta t$ con $f_S > 2f_M$.

2.2 Modello Sistema IoT

1. **Livello di campo:** sensori, attuatori e sistemi fisici;
2. **Livello di rete locale:** sistemi WPANs eWLANs di comunicazione con i sensori:
   - *WPANs:* massimo 100m, bassa velocità di trasmissione, bassi consumi, spesso non basati su IP;
   - *WLANs:* fino a qualche chilometro, spesso realizzati secondo IEEE 802.11 utilizzando protocolli IP.
3. **Livello di rete geografica:** comunicazioni che utilizzano reti LTE, CatM1, satelliti, LPWAN che utilizzano protocollo IP.
   - *Aggregatori*: consentono l'interconnessione di dispositivi con stesso protocollo a livello 2 del modello OSI;
   - *Gateway*: consentono l'interconnessione di reti con diversi protocolli a livello 2 del modello OSI;
   - *Router*: dispositivi di instradamento pacchetti IP.
4. **Livello cloud o applicazione:** fornitori di *IaaS* o *SaaS*.
   - *Analisi dei dati:* dare valore alle informazioni raccolte in massa attraverso tecniche sofisticate;
   - *Sicurezza*: riguarda l'intera architettura che costituirà la più grande superficie di attacco del pianeta.

[1] *Deltat* : intervallo di campionamento

2.3 Sistemi per IoT e Valore Atteso

Machine to Machine (M2M): Un dispositivo comunica con un altro dispositivo autonomamente2 senza protocollo IP,ma con protocolli specifici.

Supervisory Control And Data Acquisition (SCADA): Sistemi di gestione di automazioni di edifici, coinvolgono dispositivi Programmable Locic Controller (PLC) che monitorano o controllano sensori e attuatori.
A differenza di entrambi, IoT aggrega i dati verso un edge computer (o un gateway) comunicando attraverso internet, ciò consente, anche al più semplice dei dispositivi, di avere dalla sua tutto l'arsenale di tecnologie in cloud. Può aggregare nodi M2M o SCADA.

2.3.1 Leggi di Metcalfe e Backstrom

Esistono 2 leggi che regolano il valore atteso di un sistema IOT:

- **Legge di Metcalfe**: Il valore di una rete è proporzionale al quadrato degli utenti connessi. Questa legge non tiene conto della degradazione die servizi al crescere degli utenti, in assenza di un aumento di banda disponibile, di possibili utenti malevoli o di indisponibilità della rete.
- **Legge di Beckstorm**: il valore di una rete è dettato dalla somma del valore di ogni transizione generata da ognuno dei dispositivi. La formula é:

$$\sum_{i=1}^{n} V_{i,j} = \sum_{i=1}^{n} \sum_{k=1}^{m} \frac{B_{i,j,k} - C_{i,j,k}}{(1 + r_k)^{t_k}}$$

  - V_i, j: Rappresenta il valore presente del network per un dispositivo i sul network j;
  - i: Un utente individuale o dispositivo sul network;
  - j: Il network;
  - k: Una singola transazione;
  - $B_{i,j,k}$: Il beneficio che il valore k porterá al dispositivo i sul network j;
  - $C_{i,j,k}$: Il costo di una transazione k ad un dispositivo i sul network j;
  - r_k: Il tasso di sconto di interesse al tempo della transazione k;
  - t_k: Il tempo passato (in anni) per transizionare k;
  - n: Il numero di individui;
  - m: Il numero di transazioni.

Parte II

Elementi di Base

Capitolo 3

Sensori e Attuatori

Possiamo suddividerli in 3 grandi gruppi:

- **Sensori passivi:** rispondono al cambiamento dell'ambiente;
- **Sensori attivi:** inviano segnali per misurare tempo e spazio;
- **Sensori ad alte prestazioni.**

3.1 Sensori Passivi

3.1.1 Temperatura

Termocoppie : Dispositivi che non necessitano di corrente per funzionare, ma producono un segnale molto debole, dell'ordine dei microvolts (10-6V). Sfruttano l'effetto SeedBeck[1], sono formati da una coppia di conduttori, di materiale diverso, uniti in un punto nel quale viene applicata la temperatura da misurare, mentre l'altra estremità viene lasciata libera. La relazione tra i materiali e la differenza di potenziale generata, non è lineare e, per questo, sono munite di software che, facendo riferimento ad una tabella nota, è in grado di calcolarla. Vengono utilizzate in applicazioni semplici, generalmente sono poco precise poiché renderle precise richiederebbe un costo elevato, tuttavia, si comportano bene anche ad alte temperature.

Resistance Temperature Detectors (RTD): Operano in un range di temperature stretto, ma sono molto accurati; vengono raramente utilizzati per temperature oltre i 600 ∘C. Realizzati avvolgendo un filo di platino su un cilindro di materiale ceramico (o vetro) e si basano su una reazione resistenza/temperatura. Possono essere a 2, 3 o 4 fili per ottenere maggiore precisione. Richiedono una corrente di eccitazione debole per funzionare. La resistenza prodotta segue una retta con pendenza caratteristica. Spesso utilizzati in circuiti a ponte con applicazioni che linearizzano i risultati.

Termistori: Resistenze che variano la propria impedenza al variare della temperatura. Producono una grande variazione di resistenza al variare della temperatura con una relazione fortemente non lineare. Utilizzati quando è necessaria una grande accuratezza in range di temperaturemolto piccoli. Esistono di 2 tipi:

- NTC: la resistenza decresce all'aumentare della temperatura;
- PTC: la resistenza cresce all'aumentare della temperatura.

3.1.2 Corrente Elettrica

Consistono in una striscia dimetallo che viene attraversata da una corrente. Sfruttano l'effetto Hall per misurare correnti alternate o continue. Molto economici e resistenti anche in ambienti con condizioni ambientali difficili.

[1] Effetto SeedBeck: Due conduttori metallici, di materiale diverso, uniti nel punto in cui si vuole effettuare una misurazione di temperatura, generano, nel polo opposto, una differenza di potenziale che varia al variare della temperatura.

3.1.3 Luce

Fotoresistori: Semiconduttori ad alta impedenza, cioè, la resistenza decresce in funzione della luce assorbita dal semiconduttore. Sono sensibili alla lunghezza d'onda della luce incidente.

Fotodiodi: Diodi che rispondono alla luce creando una coppia elettrone-lacuna: le lacune muovono verso l'anodo, mentre gli elettronimuovono verso i catodo generando una corrente elettrica.

Pyroelectric InfraRed (PIR): Si basano su materiali sensibili alla radiazione infrarossa e al calore. Operano su lunghezze d'onda dagli 8 ai 14 micrometri, tipiche del corpo umano. Il materiale è posto dietro una **lente di Fresnel** e genera un segnale al variare del calore che attraversa la lente che viene rilevato da un transistor ed inviato ad un amplificatore. Sfruttano un valore chiamato tempo di hold che specifica il tempo per il quale l'amplificatore tiene alto il segnale, maggiore è il tempo di hold e minore è il numero di eventi che si rilevano. Si possono disporre in forma di array per effettuare misurazioni su ampie superfici.

Lente di Fresnel: Lente che raccoglie la luce o ingrandisce immagini con un ingombro minore rispetto alle lenti realizzate con geometria tradizionale. Sono composte da una serie di scalanature concentriche strette sulla superficie di un foglio di plastica leggero (al fine di ridurre lo spessore, il peso e il costo). Ogni scalanatura ha un'angolazione leggermente diversa dalla successiva, ma con la stessa lunghezza focale così da focalizzare la luce tutta in un punto centrale. Un'elevata densità di scalanature corrisponde ad un'immagine di qualità migliore.

3.2 Sensori Attivi

3.2.1 Sensori Light Detection And Ranging (LiDAR):

Misurano la distanza di un obiettivo basandosi sul "tempo di volo" di un impulso laser riflesso da un target. Sono in grado di analizzare qualunque cosa attraversi l'impulso. I laser lavorano su lunghezze d'onda da 600 a 1000 nanometri o oltre i 1550 nanometri (per evitare danni agli occhi) e sono relativamente economici. Il segnale di ritorno viene rilevato da una batteria di fotodiodi che calcola il tempo di volo.

3.2.2 Sensori Micro ElectroMechanical System (MEMS):

Sensori che incorporano strutture meccaniche miniaturizzate che interagiscono con componenti elettronici, alterando la propria forma e generando un segnale elettrico. Tra i dispositivi MEMS abbiamo:

- **Accelerometro:** Sensore MEMS che risponde ad un cambiamento di velocità lineare, si basa sul fatto che un dispositivo piezoelettrico produce una differenza di potenziale in risposta ad un movimento.Ha una piccola massa tenuta da molle, il movimento produce uno spostamento della massa che fa variare la capacità del circuito interno; questa variazione può essere misurata.
- **Giroscopio:** Formato da dei dischi di silicio che, se messi in rotazione dalle forze di Coriolis[2], fanno variare la capacità del circuito.
- **Microfono:** Rileva suoni o vibrazioni, molto utilizzato in industria per prevenire malfunzionamenti o incidenti.
- **Sensori di pressione:** Misurano la pressione di liquidi e gas, il cuore del circuito è un piezoelettrico che, cambiando forma, produce una differenza di potenzialemisurabile.

3.3 Sensori ad Alte Prestazioni

Sono sensori con capacità elevate di calcolo, noi parleremo dei sistemi di visione le cui componenti principali sono:

[2]Forza di Coriolis: forza fittizia in cui un oggetto sembra essere soggetto a una forza laterale, anche se non vi è alcuna forza applicata esternamente.

1. Un sistema ottico;
2. Circuiti sensibili alla luce.

I circuiti sensibili alla luce si dividono in:

- **Charge Coupled Devices (CCD):** Generano immagini ad alta risoluzione e con poco rumore, consumano però tanta energia ed inoltre richiedono complicati processi di produzione.
- **ComplementaryMetal Oxide Semiconductor (CMOS):** Ogni pixel è costituito da un transistor miniaturizzato che viene letto in maniera indipendente. Molto sensibile al rumore, ma molto economico in termini di energia e costi di produzione. Solitamente organizzati in matrici bidimensionali, con transistor sensibili su cui microlenti fanno convergere l'immagine da riprendere. Largamente utilizzati per controlli di qualità nell'industria.

3.4 Integrazione di Sensori

Operazione che consente di utilizzare più tipi di sensori per rivelare informazioni più complesse attraverso due metodologie principali:

1. *Centralizzato*: i dati vengono fatti convergere in un unico punto e lì elaborati;
2. *Decentralizzato*: i dati sono elaborati a bordo dei sensori.

Capitolo 4

Sorgenti ed Accumulatori di Energia

La gestione del consumo dell'energia coinvolge sia hardware che software e riguarda principalmente:

- Energia assorbita da sensori, microcontrollori ed eventuali sistemi di comunicazione;
- Frequenza di campionamento;
- Perdite dovute all'inefficienza delle batterie.

Nel caso delle batterie, non abbiamo un comportamento lineare nel tempo ed i dispositivi alimentati possono avere comportamenti del tipo: se il voltaggio di alimentazione cala, il microprocessore potrebbe non raggiungere la soglia di operatività e non essere più in grado di funzionare.

Gestione dell'assorbimento: Esistono diverse pratiche per ottimizzare il consumo di energia, come il Clock gating, cioè ridurre il clock delle componenti non utilizzate.

4.1 Approvvigionamento di Energia

I sistemi possono produrre energia quando cambiano stato, temperatura, illuminazione o vengono attraversati da un'onda elettromagnetica. Alcuni dispositivi sfruttano questa energia prodotta come unica fonte. Tra i diversi metodi di approvvigionamento energetico esistono:

- **Energia solare:** Energia proveniente dalla luce, naturale o artificiale, catturata attraverso delle matrici di fotodiodi aggregate insieme sotto il nome di pannelli solari. L'energia prodotta è in funzione della quantità di luce incidente. Non sono, in genere, molto efficienti, hanno prestazioni che variano tra l'8 e il 20%, con una media del 12%, ma solo con un'incidenza perpendicolare della luce.
- **Energia prodotta da dispositivi piezo-meccanici, elettrostatici o elettromagnetici:** Attraverso sensori MEMS si genera energia da movimento, vibrazioni e suoni. Energia prodotta nell'ordine dei milliwatt, adatta a dispositivi molto piccoli.
- **Energia da Radio Frequenza:** Sfruttano l'onda elettromagnetica incidente su di essi per generare energia. Gli stessi Radio Frequency Identification (RFID), essendo piazzati su oggetti utilizzati per ricevere ed inviare onde radio, beneficiano di questo traffico per produrre energia. Per altre applicazioni, si sfrutta l'energia prodotta da emittenti broadcast. Produce una bassissima quantità di energia.
- **Energia da gradienti termici**: Attraverso una differenza di temperatura:
  - Sfruttando **fenomeni termoelettrici** (effetto Seebeck): Si sfruttano delle termocoppie chiamate *ThermoElectric Generator (TEG)*. L'energia prodotta è proporzionale a quadrato della differenza di potenziale e proporzionale alla differenza di temperatura tra i 2 elettrodi. Le termopile sono serie di termocoppie di cui viene sommata la differenza di potenziale. Sono dispositivi molto piccoli, poco costosi e duraturi nel tempo, tuttavia, non producono una grande quantità di energia.

  - Sfruttando **fenomeni termoionici** (effetto thermotunneling) : Si basano sul fenomeno fisico per cui gli elettroni vengono espulsi da un elettrodo caldo verso uno freddo, sfondando una barriera di potenziale. L'energia richiesta per fare ciò è direttamente proporzionale alla differenza di temperatura tra i due elettrodi, spesso così elevata da non essere adatti per il campo IoT.

- **Energia da radioattività:** L'energia radioattiva ad elevate densità, produce energia termica dall'energia cinetica delle particelle. L'energia prodotta è nell'ordine dei kilowatt. Il problema principale è che il decadimento radioattivo ha un profilo di densità di potenza molto debole. Un ulteriore problema è relativo alla necessità di ricorrere a schermature in piombo aumentando il peso e il costo dei dispositivi.

4.2 Accumulatori di Energia

La capacità viene misurata in Ampere all'ora. Le stime sulla durata di una batteria si basano sull'**effetto Peukert**: la capacità di una batteria decresce a velocità diverse quando si incrementa la scarica, cioè scaricando velocemente una batteria, viene rimossa maggiore capacità rispetto alla scarica lenta della stessa.

Curve di scarico: A seconda del materiale che compone la batteria, si possono avere differenti curve di scarico:

- *Alcaline:* andamento lineare per un grande range di scarica;
- *Ioni di Litio:* andamento lineare, ma presentano uno scalino in prossimità della scarica completa, che rende imprevedibile il punto dove avverrà ciò;
- *Nichel Cadmio:* meno differenza di potenziale, ma un andamento di scarica curvilineo facilmente prevedibile.

Diagramma di Ragone: È disegnato in scala logaritmica, dove vengono confrontate la densità di energia di una sorgente e la densità di potenza; inoltre, mostra anche il tempo di scarica. Evidenzia i dispositivi che durano più a lungo rispetto a quelli che immagazzinano più energia.

Batterie alcaline: Utilizzate in applicazioni che assorbono molta corrente; perfetta per applicazioni a basso assorbimento di corrente, tuttavia ha un costo elevato.

Batterie agli ioni di Litio: Alta densità di energia data dal movimento fisico degli ioni di litio tra gli elettrodi. Dopo una serie di cicli carica/scarica, inizia a subire un effetto memoria che comporta perdita di capacità. La temperatura influisce sulla perdita di capacità. Le reazioni chimiche indesiderate influiscono negativamente sulla perdita di capacità. La perdita minima della capacità corrisponde a circa il 2% al mese.

Supercondensatori: Immagazzinano grandi volumi di energia, hanno densità di energia tipica delle batterie. Sono costruiti con materiali "esotici" che impattano sul costo, tuttavia si caricano in pochi secondi. L'energia è immagazzinata su una piastra e quindi non è coinvolto nessun processo chimico; inoltre, non possono essere sovraccaricati e si presentano in 2 forme:

1. *Condensatori a doppio strato:* utilizzano carbone attivo e trasferiscono carica elettrostaticamente;
2. *Pseudocondensatori:* utilizzano un metallo e trasferiscono carica in maniera elettrochimica. L'energia rimanente può essere dedotta dal cambiamento di differenza di potenziale ai poli che, cambiando costantemente, ci da informazioni sullo stato di scarica.

Parte III

Tecnologie per la Comunicazione

Capitolo 5

Non Basate su Protocollo IP

Dominio della PAN a corto raggio, attraverso cavi o wireless. La WPAN è il metodo prevalente, il cavo viene utilizzato solo in zone in cui il segnale è molto disturbato. Gli **standard 802.15** nascono per studiare dispositivi PAN, ma si sono espansi e ora si concentrano su protocolli per l'alta velocità di trasmissione.

5.1 Bluetooth

Tecnologia di collegamento wireless a basso consumo. Bluetooth Special Interest Group: organizzazione che sovrintende lo sviluppo degli standard Bluetooth. Molto utilizzato nel mondo IoT, soprattutto la versione *Low Energy* (LE), grazie alla lungimiranza del progetto iniziale e al tipo di licenza, poiché open source.

5.2 ZigBee

Protocollo per WPAN basato su IEEE 802.15.4[1] indirizzato alla rete IoT per ambito commerciale dove abbiamo vincoli di costo, ingombro e alimentazione. Trasporta pacchetti in una rete mesh[2]. Opera nelle frequenze radio di 2.4GHz ed è una tecnologia nata per essere più semplice ed economica di Bluetooth, prima dell'avvento di Bluetooth LE. È uno standard proprietario e chiuso che richiede il pagamento di una licenza per l'utilizzo. Non offre un servizio di trasporto dati, ma è in grado di formare e gestire una rete.

5.2.1 Architettura

Composta da 3 elementi principali:

- **ZigBee Controller (ZC):** dispositivo con buone capacità computazionali, utilizzato per formare la rete iniziale. Ogni rete ha un controller e, dopo la creazione della stessa, questo diventa un router. Assegna indirizzi di rete logici e consente agli altri dispositivi di unirsi alla rete o abbandonarla;
- **ZigBee Router (ZR):** componente opzionale che alleggerisce il carico della rete mesh. Partecipa all'instradamento multi-hop dei messaggi e consente agli altri dispositivi di unirsi alla rete o abbandonarla;
- **ZigBee End Device (ZED):** dispositivo endpoint con la capacita di comunicare, ma non ha logiche di instradamento e non può gestire autonomamente l'associazione alla rete.

La comunicazione avviene in 3 distinte modalità:

- **Dati ciclici o periodici:** dati inviati ad intervalli di tempo regolari;
- **Dati ciclici a bassa latenza:** dati inviati in finestre temporali che possono avere latenze molto basse;

[1] IEEE 802.15.4: protocollo per le reti di sensori a basso consumo e corto raggio.

[2] Rete mesh: tipo di rete di in cui ogni dispositivo è collegato direttamente agli altri dispositivi all'interno della rete e può fungere da nodo di trasmissione e/o ricezione dei dati, senza la necessità di un'infrastruttura centralizzata.

- **Dati intermittenti:** dati inviati quando viene generato un evento esterno.

Esistono 3 topologie di base:

- **Rete a stella:** un solo ZC con ZED periferici e quindi un solo salto. Distanza massima tra ZED e ZC limitata e lo ZC rappresenta l'unico punto di fallimento;
- **Rete ad albero:** rete multi-hop che impiega segnalazioni. ZC e ZR posso avere figli e gli ZED rappresentano le foglie dell'albero. Ogni nodo, ad eccezione degli ZED, può comunicare sia verso i genitori che verso i figli. Gli ZED possono comunicare solo verso i genitori. Il centro rappresenta l'unico punto di fallimento;
- **Rete a maglia:** i percorsi vengono stabiliti in maniera dinamica e la comunicazione può avvenire da e verso qualunque nodo utilizzando algoritmi di instradamento basati su tabelle.

I nodi possono essere attivati in qualunque momento producendo un notevole consumo di energia. La latenza diventa non deterministica. Tuttavia, può crescere in maniera indefinita e non ci sono grandi punti critici.

Come si associa un nuovo dispositivo: Viene inviata una richiesta broadcast a tutti i dispositivi autorizzati, chiedendo di inviare, a loro volta, un segnale di conferma. Inizialmente solo lo ZC risponderà, successivamente anche gli ZR. Subito dopo avverrà la procedura di associazione.

Sicurezza: Implementa 3 diversi meccanismi di sicurezza: ACLs, cifratura 128-bit AES e marcatori di durata del messaggio. Sicurezza distribuita su 3 livelli dello stack OSI:

- *Livello applicazione:* creazione delle chiavi;
- *Livello rete:* utilizzo di una chiave definita dall'instradamento;
- *Livello collegamento:* gestita tramite API.

Sfrutta 3 diversi tipi di chiavi:

- *Master Key:* preinstallata dal costruttore o inserita manualmente;
- *Network Key:* utilizzata nel livello rete;
- *Link Key:* garantisce l'associazione tra due dispositivi.

5.3 Zwave

Tecnologia WPAN che opera sulle frequenze di 900MHz utilizzata per l'automazione domestica. Protocollo proprietario tutt'ora largamente non divulgato, con il vincolo di usare poca banda per comunicare con sensori e interruttori. Si basa su specifiche International Telecommunications Union (ITU) per comunicare a corto raggio in banda stretta. Può operare a 3 velocità:

- 100Kbps a 916MHz con estensione di 400KHz;
- 40Kbp a 916MHz con estensione di 300KHz;
- 9.6Kbp a 908MHz con estensione di 300KHz.

I nodi della rete sono:

- *Controller Device:* dispositivo di alto livello che controlla la tabella di routing della rete; ne esistono di due tipi:
  - *Primario*: ne può esistere solo uno, mantiene la topologia e la gerarchia della rete includendo ed escludendo nodi assegnandogli il loro ID;
  - *Secondario*: assiste il controller primario negli instradamenti.
- *Nodi o Slave*: dispositivi che eseguono azioni in base ai comandi ricevuti. Non possono comunicare se non gli viene richiesto. Possono memorizzare informazioni di instradamento ma non hanno tabelle. Operano come fossero dei ripetitori.

Indirizzamento: Molto più semplice di Bluetooth e ZigBee, progettato con lo scopo di minimizzare il traffico ed i consumi. Ci sono 2 identificatori:

- *Home ID*: indirizzo di 32 bit pre-programmato che identifica la rete;
- *Node ID*: indirizzo di 8 bit assegnato dai controller ai nodi.

Quando un nuovo dispositivo vuole entrare nella rete, avvia una procedura di accoppiamento e aggiunta invocando il controller primario che gli assegnerà un Home ID + Node ID.

Instradamento: Un singolo controller primario gestisce la rete e stabilisce gli instradamenti. Sfrutta una tabella molto semplice poiché indica solo i vicini dei nodi distanti solo un salto. Il controller aggiorna la tabella chiedendo informazioni ai nodi. Quando un nodo riceve un pacchetto non suo, lo inoltra al nodo successivo.

5.4 Sistemi Heading Ventilation Air Conditioning (HVAC)

Progettati ed utilizzati per il controllo e il monitoraggio dei sistemi di combustione, riscaldamento, ventilazione e condizionamento dell'aria. Si basano sulla progettazione, lo sviluppo e la fornitura di componenti hardware e software con un elevato livello di connettività e digitalizzazione, garantendo il risparmio energetico e misurando i consumi. Grazie all'IoT, questi sistemi sono stati collegati a delle applicazioni che permettono, all'utente finale, una gestione completa dell'impianto in tempo reale.

5.4.1 Sistemi Building Management System (BMS)

Sistemi di controllo centralizzato di tutte le apparecchiature meccaniche ed elettriche in un edificio. HVAC rappresenta l'elemento più complesso di tutto il BSM. Consente di comprendere meglio il funzionamento di un edificio ed effettuare opportune modifiche in modo da ottimizzare il flusso di operazioni e ridurre i consumi energetici; inoltre, consente di diagnosticare eventuali guasti e malfunzionamenti a distanza. L'integrazione nel cloud permette la comunicazione tra diversi sistemi.

Sistemi di riscaldamento: Assumono forme diverse, alcuni bruciano materiale per fornire aria riscaldata, altri riscaldano l'acqua facendola passare in circuiti appositi, generalmente funzionano a gas naturale o propano. Un'altra opzione è il pavimento radiante che utilizza tubazioni sottopavimento costituite da tubi flessibili che vengono riempiti con acqua o con una soluzione gliconica.

Sistemi di raffreddamento: Gli elementi interni ed esterni di questi sistemi devono essere completamente collegati, sono relativamente economici e si possono montare in autonomia. PEr i climi secchi si usano raffreddatori evaporativi che attirano l'acqua esterna nel sistema, facendola passare attraverso cuscinetti saturi d'acqua che inumidiscono e rinfrescano l'aria prima di introdurla nell'ambiente.

5.5 KONNEX

Noto anche come KNX, è uno standard per l'automazione degli edifici. È un protocollo di comunicazione open-source che consente la gestione e il controllo di una vasta gamma di dispositivi e sistemi all'interno di un edificio. Le caratteristiche principali sono:

- *Interoperabilità*: i dispositivi KNX possono comunicare tra loro e lavorare in sinergia senza problemi, indipendentemente dal produttore;
- *Cablaggio*: utilizza una topologia a bus, in cui tutti i dispositivi KNX sono collegati a un unico bus di comunicazione, semplificando l'installazione e il cablaggio dei dispositivi, riducendo i costi e semplificando la manutenzione;
- *Controllo flessibile*: e personalizzabile degli impianti dell'edificio tramite sistemi intuitivi;
- *Gestione dell'energia*: attraverso funzionalità avanzate;
- *Espandibilità*: è possibile aggiungere nuovi dispositivi senza dover sostituire l'intero sistema.

Capitolo 6

Basate su Protocollo IP

Indipendentemente dai sensori, il dato giungerà al cloud per essere analizzato. Dal punto di vista IoT, avvicinare il protocollo IP ai dati consente di collegare IT e OT. Vantaggi di IP:

- Onnipresente in quasi tutti i sistemi operativi e su sitemi WPAN;
- Longevo poiché ha oltre 40 anni;
- Basato su standard;
- Scalabile dato che IPv6 potrebbe fornire indirizzi IP univoci ad ogni atomo del globo;
- Gestibile grazie ai vari strumenti;
- Affidabile poiché la consegna del pacchetto è sempre garantita.

IP sfrutta il metodo di consegna "best-effort" che permette di trasmettere pacchetti attraverso più percorsi, scegliendo il migliore, consentendoci di sostituire i livelli 1 e 2 senza modificare i pacchetti e avendo la certezza che questi vengano comunque consegnati. IP necessita un livello di rete ben supportato e ciò avviene anche grazie ai protocolli TCP (orientato alla connessione) e UDP (non orientato alla connessione). UDP è più semplice da implementare ma non resiliente. TCP tuttavia fornisce meccanismi di controllo del flusso. Entrambi forniscono procedure di riordino dei segmenti.

Gli enti da menzionare nel campo della tecnologia e comunicazione sono:

- International Standard Organization (ISO): Principale ente internazionale di standardizzazione, che si occupa anche di tecnologia e reti.
- Institute of Eletrical and Electronics Engineers (IEEE): Organizzazione mondiale degli ingegneri elettrici ed elettronici.

6.1 Modello OSI

Il Modello OSI é il progetto di riferimento per le reti di calcolatori, con un approccio a 7 livelli, ciascuno con una specifica funzione:

1. *Livello Fisico* [Bit]: mezzo, segnale e trasmissione binaria;
2. *Livello Collegamento* [Trame]: indirizzamento fisico (MAC e LLC);
3. *Livello Rete* [Pacchetti]: determinazione dei percorsi e indirizzamento logico (IP);
4. *Livello Trasporto* [Segmenti]: connessioni end-to-end e affidabilitá;
5. *Livello Sessione* [Dati]: comunicazione inter-host;
6. *Livello Presentazione* [Dati]: rappresentazione dei dati e criptazione;
7. *Livello Applicazione* [Dati]: dal processo di rete all'applicazione.

Dal primo al terzo livello si tratta di livelli dei mezzi, mentre i rimanenti sono i livelli degli host.

Progetto IEEE 802 (Ethernet): Inserito nel modello OSI ai livelli 1 e 2 per LAN e WAN, ha prodotto una serie di standard ed è suddiviso in molteplici gruppi.

Protocollo IP: Inserito nel modello OSI al livello 3, definisce un meccanismo di consegna dati di tipo non affidabile e non orientato alla connessione. Ogni pacchetto IP può essere suddiviso in *Header IP* e *DATA*. L'Header IP contiene, tra gli altri campi, indirizzo di mittente e destinatario. Prevede la consegna a 3 tipi diversi di destinatari:

1. *Unicast delivery:* singolo destinatario;
2. *Broadcast delivery:* tutti gli utenti di una rete;
3. *Multicast delivery:* un sottogruppo di utenti di una rete.

6.2 Sistemi Wireless: Diagrammi di Irradiazione Antenne

6.2.1 Antenna Isotropica (Diagramma di Radiazione)

L'antenna isotropica teorica rappresenta un punto infinitamente piccolo nel vuoto, radiante idealmente uniformemente in qualsiasi direzione dello spazio, senza riflessioni e perdite (il suo diagramma di radiazione è una sfera). Per calcolare il guadagno in potenza di un'antenna espresso in dBi, si usa la seguente formula

$$G(dBi) = 10 \cdot \log_{10}(G) = 10 \cdot \log_{10}\left(\frac{P}{P_i}\right)$$

Dove:

$$P = \text{potenza della antenna in esame}$$

$$P_i = \text{potenza della antenna isotropica}$$

$$G(dBi) = \text{guadagno di un'antenna rispetto a un'isotropica, espresso in decibel}$$

L'antenna isotropica ha un guadagno di 0 dBi. Convertendo in scala lineare si ottiene:

$$G = 10^{\frac{G(dBi)}{10}}$$

L'unità dBi e il termine "antenna isotropica" vengono utilizzati per calcolare $E.I.R.P.$ (Effective Isotropic Radiated Power).$EIRP$ rappresenta la potenza che dovrebbe essere irradiata da un'antenna isotropica ipotetica per ottenere lo stesso livello di segnale nella direzione di radiazione massima di un'antenna. Viene utilizzato nella progettazione e nei calcoli dei parametri delle reti Wi-Fi, collegamenti satellitari, ecc.

La normativa vigente dell'Unione Europea stabilisce la potenza massima a cui è consentita la trasmissione in una gamma di frequenza Wi-Fi:

- $2400,0 - 2483,5$ MHz (banda a $2,4$ GHz) - la potenza non può superare i 100 mW $E.I.R.P.$ (20 dBm);
- $5150 - 5350$ MHz (banda a 5 GHz) - la potenza non può superare i 200 mW $E.I.R.P.$ (23 dBm);
- $5725 - 5875$ MHz (banda a 5 GHz) - la potenza non può superare i 1000 mW $E.I.R.P.$ (30 dBm).

Ricordiamo che i produttori dei punti di accesso (Access Points) spesso indicano la potenza del trasmettitore in $E.I.R.P.$. Ciò significa che il dispositivo è conforme alle normative solo ed esclusivamente con antenna fornita in dotazione o antenna integrata. Se si decide di costruire un dispositivo Wi-Fi, è necessario fare semplici calcoli per verificare se ci si trova all'interno della gamma di potenza consentita dalla legge.

Per calcolare $E.I.R.P.$ di un sistema costituito da un trasmettitore (ad esempio, router wireless), cavo e antenna, si utilizza la seguente formula:

$$E.I.R.P. = P - l \cdot Tk + Gi$$

Dove:

$$P = \text{potenza del trasmettitore espressa in dBm}$$

$$l = \text{lunghezza del cavo in metri}$$

$$Tk = \text{attenuazione di 1 metro di cavo alla frequenza di lavoro del trasmettitore}$$

$$Gi = \text{guadagno in potenza di un'antenna isotropica espresso in decibel}$$

Attenzione che non tutti i punti di accesso sono in grado di ridurre la potenza di uscita e quindi il guadagno di antenna diventa il solo parametro modificabile. In generale è consigliabile utilizzare un'antenna con alto guadagno e un trasmettitore con meno potenza rispetto a un'antenna con basso guadagno e un trasmettitore con più potenza perché i dispositivi non funzionano solo in trasmissione ma anche in ricezione e quindi la sensibilità del ricevitore è importante.

6.2.2 Diagrammi di Irradiazione

L'irradiazione è il termine usato per rappresentare l'emissione o la ricezione del fronte d'onda dell'antenna, specificandone l'intensità. In ogni progetto RF si può notare sempre un particolare grafico che rappresenta la radiazione dell'antenna. Esso è il diagramma di radiazione e permette facilmente di risalire alle caratteristiche e alla direttività di un'antenna. Un diagramma può contenere i seguenti lobi:

- **Lobo di radiazione principale:** è il picco più intenso della radiazione. Questa è la parte in cui esiste la massima energia irradiata. La direzione di questo lobo indica la direttività dell'antenna;
- **Lobo minore:** qualsiasi lobo di radiazione diverso dal lobo principale;
- **Lobo laterale:** è il lobo di radiazione in qualsiasi altra direzione diversa da quella prevista;
- **Lobo posteriore:** è il lobo di radiazione opposto a quello principale. Qui si spreca una notevole quantità di energia.

6.3 IEEE 802.11

L'IEE 802.11 é un suit di protocolli che definisce il Media Access Controll (MAC) e il livello fisico di uno stack di rete. Wi-Fi è la definizione di WLAN basata sugli standard IEEE 802.11. La sostituzione dei livelli 1 e 2 con i livelli IEEE 802.11, ha consentito di utilizzare facilmente la struttura TCP/IP esistente. Inizialmente si basava su sicurezza *Wired Equivalent Privacy* (WEP) che si è rivelata inaffidabile e compromettibile, sostituita poi da *Wi-Fi Protected Access* (WPA) e WPA2 che utilizzano chiavi a 256 bit. Il protocollo IEEE 802.11 rappresenta una famiglia di comunicazioni radio basate su tecniche di modulazione nelle bande senza licenza a 2.4GHz e 5GHz. Supporta 3 tipologie:

- **Basic Service Set (BSS)**:questa topologia a stella è formata un dispositivo endpoint (STA) che comunica con un punto di accesso (AP) che può essere un gateway per altre reti o un router;
- **Indipendent Basic Service Set (IBSS)**: in questa topologia peer-to-peer ciascun endpoint comunica con altri endpoint, non viene realizzato nessun AP;
- **Sistema distribuito**: combina due o più reti IBSS collegandole attraverso degli AP e consente di avere fino a 2007 endpoint collegati.

Tecniche di modulazione e codifica: Permettono di trasformare i segnali da digitali ad analogici e viceversa. Un segnale portante[1] analogico viene modulato in discreto formando quello che viene chiamato simbolo. Ci sono 3 forme base di codifica dei simboli:

- *Amplitude Shift Keying (ASK)*: l'informazione viene rappresentata mediante variazioni dell'ampiezza del segnale portante. Il segnale modulante viene moltiplicato per la portante, generando una nuova forma d'onda modulata;

[1]Segnale portante: è una forma d'onda di base a una frequenza costante e stabile che viene modulato per trasportare informazioni.

- *Frequency Shift Keying (FSK)*: l'informazione viene codificata mediante variazioni della frequenza del segnale portante. Le variazioni della frequenza sono proporzionali all'informazione da trasmettere;
- *Phase Shift Keying (PSK)*: l'informazione viene codificata mediante variazioni della fase del segnale portante. La fase rappresenta il punto di inizio dell'onda. Le variazioni della fase del segnale portante rappresentano l'informazione da trasmettere.

Solitamente indicata con una notazione numerica a seconda del numero di simboli distinti utilizzati. Ad esempio, PSK-2, noto anche come Binary Phase Shift Keying (BPSK), utilizza due simboli con una differenza di fase di 180 gradi, mentre PSK-4, utilizza quattro simboli con differenze di fase di 90 gradi.

Tecniche di modulazione dell'interferenza:

- *Frequency Hopping Spread Spectrum (FHSS)*: tecnica in cui il segnale viene suddiviso in pacchetti e trasmesso su diverse frequenze nel tempo con rapidi cambiamenti di frequenza secondo una sequenza predefinita;
- *Direct Sequence Spread Spectrum (DSSS)*: tecnica in cui il segnale viene espanso o "spalmato" su una banda di frequenza più ampia rispetto a quella richiesta per la trasmissione dei dati, moltiplicando il segnale con una sequenza pseudocasuale chiamata codice di spargimento;
- *Orthogonal Frequency Division Multiplexing (OFDM)*: tecnica che suddivide il segnale in una serie di sottoportanti ortogonali, ciascuna trasportando una porzione del segnale, organizzate in modo che non si sovrappongano tra loro, riducendo l'interferenza interportante. Le sottoportanti possono essere collocate vicine l'una all'altra senza causare interferenza.

6.4 IEEE 802.11 Multiple Input, Multiple Output (MIMO)

Sfrutta un fenomeno chiamato multipath che implica la riflessione dei segnali su delle superfici, così che il ricevitore riceve più volte lo stesso segnale in momenti diversi attraverso percorsi diversi. Tuttavia, il multipath distorce i segnali e causa interferenze che degradano la qualità del segnale. Con l'aggiunta di più antenne si può aumentare linearmente la capacità di un canale. Esistono due forme di MIMO:

- **Diversità spaziale**: un singolo flusso di dati trasmesso su più antenne contemporaneamente utilizzando la codifica spazio-temporale fornendo miglioramenti nel rapporto segnale-rumore e miglioramenti nell'affidabilità del collegamento e della copertura del sistema. L'utilizzo di più flussi incide sul consumo energetico effettivo;
- **Multiplexing spaziale**: utilizzato per fornire più capacità di dati utilizzando percorsi multipli per trasportare traffico aggiuntivo dividendo un singolo flusso di dati in più trasmissioni separate su diverse antenne.

6.4.1 IEEE 802.11n

Consente quattro antenne e quattro flussi spaziali offrendo connessioni ad alta velocità. Utilizza modulazione OFDM e MIMO per migliorare le prestazioni. Supporta canali larghi fino a 40MHz, consentendo una maggiore velocità di trasmissione. L'aggregazione dei pacchetti combina più pacchetti in un unico frame, migliorando l'efficienza. Il beamforming[2] dirige il segnale verso il destinatario, migliorando la copertura. Offre prestazioni superiori, velocità più elevate e una migliore affidabilità delle connessioni wireless.

6.4.2 IEEE 802.11ac (Wi-Fi 5)

WLAN di nuova generazione, è uno standard di comunicazione wireless che offre prestazioni avanzate rispetto agli standard precedenti. Alcune caratteristiche principali:

- *Velocità elevata:* utilizzando canali larghi 80MHz o 160MHz, con velocità teoriche maggiori di 1Gbps;

[2]Beamforming: tecnica che dirige in modo selettivo il segnale wireless verso un destinatario specifico, migliorando la portata, la qualità del segnale e la velocità di trasmissione.

- *MIMO multi-stazione:* la tecnologia MIMO multi-stazione (MU-MIMO), consente all'access point di comunicare contemporaneamente con più dispositivi wireless, migliorando l'efficienza dello spettro e consentendo una maggiore capacità di rete;
- *Modulazione 256-QAM:* vengono utilizzati 256 livelli di ampiezza e fase per rappresentare combinazioni di bit, consentendo di trasmettere una grande quantità di dati;
- *Beamforming esplicito:* consente di indirizzare il segnale wireless in modo mirato verso i dispositivi client, migliorando la copertura e la qualità del segnale;
- *Retrocompatibilità:* i dispositivi possono connettersi a reti wireless che utilizzano standard antecedenti.

6.4.3 IEEE 802.11p

Noto anche come Wireless Access in Vehicular Environments (WAVE), è uno standard sviluppato specificamente per le applicazioni di comunicazione veicolare. Opera nella banda di frequenza dedicata ai servizi di comunicazione per veicoli a 5,9GHz. Le caratteristiche principali sono:

- *Comunicazione veicolare:* comunicazione tra veicoli (V2V) e tra veicoli e infrastrutture (V2I), portando a scambio di informazioni stradali;
- *Basso ritardo di trasmissione:* consentendo una comunicazione quasi in tempo reale tra i veicoli, caratteristica fondamentale per applicazioni critiche per la sicurezza stradale;
- *Copertura estesa:* consentendo una comunicazione affidabile su lunghe distanze e permettendo una comunicazione efficace tra veicoli che si trovano a diversi metri di distanza;
- *Tolleranza alle interferenze:* garantisce comunicazione affidabile in presenza di rumore e ostacoli fisici.
- *Rete non strutturata:* non esiste una gerarchia o una struttura organizzata predefinita tra i nodi di rete che comunicano direttamente tra loro senza passare attraverso un punto centrale di controllo;
- *Rete spontanea:* si forma in modo automatico senza un'organizzazione predefinita.

Inolte, la larghezza del canale è di 10MHz e opera nella larghezza di banda di 75MHz. Utilizza gli schemi classici di modulazione e non è necessario l'impiego di tecniche come MIMO o beamforming.

6.4.4 IEEE 802.11ah

Noto anche come Wi-Fi HaLow, è uno standard sviluppato per supportare reti a bassa potenza e lungo raggio, ottimizzate per applicazioni a basso consumo energetico. Le caratteristiche principali sono:

- *Frequenza di operazione:* opera nella banda di frequenza a 900MHz, che offre una migliore capacità di penetrazione degli ostacoli e una maggiore copertura rispetto alle bande di frequenza più alte;
- *Copertura estesa:* comunicazione su distanze più lunghe rispetto agli standard Wi-Fi convenzionali;
- *Consumo energetico ridotto:* progettato per ridurre al minimo il consumo energetico, ottimizzando le prestazioni per dispositivi a batteria e applicazioni a basso consumo energetico;
- *Larghezza di banda ridotta:* offre una maggiore efficienza spettrale per supportare un gran numero di dispositivi connessi simultaneamente;
- *Scalabilità:* consente la gestione di un gran numero di dispositivi all'interno di una singola rete senza compromettere le prestazioni complessive.

Esistono 3 tipi di stazioni:

- **Radice**: funge da gateway per le altre reti;
- **STA**: stazione tipica della 802.11;
- **Nodo di inoltro**: combina gli AP con le STA che si trovano su un BSS inferiore fornendogli un'interfaccia di comunicazione.

Ogni stazione viene aggiornata attraverso dei beacon[3] inviati dagli AP, attraverso un timer (chiamato Target Wait Time TWT) che gli permetterà di risvegliarsi unicamente per ricevere i beacon o inviare informazioni. Inoltre, essendo presenti tante stazioni, la bitmap viene segmentata e i beacon ne trasportano delle porzioni. 802.11 ah utilizza un valore che indica il periodo di inattività massimo, nei protocolli standard 802.11, questo valore a 16 bit può garantire massimo 16 ore di inattività; ma in queste reti i primi due bit sono un fattore di scala consentendo un periodo di inattività fino a 5 anni.

6.5 6LoWPAN

Il nome sta per IPv6 su reti personali wireless a bassa potenza. L'intento è realizzare reti basate su IP su sistemi di comunicazione in radio frequenza a bassa potenza per dispositivi limitati in termini di alimentazione e spazio che non necessitano di servizi di rete a larghezza di banda elevata. Necessitano di un router edge in grado di:

- Gestire la comunicazione tra i nodi;
- Trasmettere dati su internet;
- Comprimere le intestazioni IPv6 a 40B e le intestazioni UDP a 8B;
- Avviare la rete.

Topologie: I router edge formano reti mesh e possono mediare scambi di informazioni tra IPv6 e IPv4. Tutti i nodi condividono lo stesso prefisso IPv6 prestabilito dal router edge. Esistono 3 tipi di nodi:

- *Nodi router:* instradano i pacchetti i permettono a più reti di comunicare;
- *Nodi host:* endpoind che consumano e producono dati;
- *Router edge.*

I nodi sono liberi di spostarsi tra le varie reti mesh associandosi continuamente a router edge diversi.

Sicurezza: Al livello 2 si basa sulla crittografia dei dati AES-128, al livello 3 ha la possibilità di usare lo standard IPsec.

6.5.1 Thread

Protocollo di rete che si basa su 6LoWPAN con obiettivo la connettività domestica e la domotica. Si basa sui livelli forniti da 802.15.4 e sulla sicurezza e il routing di 6LoWPAN. A differenza di altri protocolli, il sensore Thread non ha bisogno di mantenere lo stato dell'applicazione, risparmiando energia al sistema. Funziona a 250Kbps nella banda GHz e stabilisce le comunicazioni attraverso i router di frontiera. Esistono 5 tipi diversi di ruoli:

- **Router di frontiera:** è un gateway e forma il punto d'ingresso a internet;
- **Dispositivo leader:** festisce un registro di ID dei router, controlla le richieste dei dispositivi REED da promuovere a router, può fungere da router e assegna gli indirizzi attraverso il Constrained Application Protocol (CoAP);
- **Thread router**: gestiscono il routing e non si sospendono mai, possono essere degradati a REED;
- **REED**: dispositivo host che può diventare un router o un leader;
- **End devices:** dispostivi host che non possono diventare router, di dividono in:
  - *Final End Device (FED);*
  - *Minimal End Device (MED);*
  - *Inactive End Device:* sospesi e comunicano solo con il router associato.

[3]Beacon: pacchetto di segnalazione periodico trasmesso da un punto di accesso per annunciare la presenza e le informazioni di base sulla rete.

Capitolo 7

Sistemi e Protocolli di Comunicazione a Lungo Raggio

7.1 Rete cellulare

Forma di comunicazione più diffusa, inizialmente, i dispositivi di comunicazione mobile avevano una copertura limitata, uno spazio di frequenza condiviso ed erano radio a due vie. Ad oggi si sfrutta il modello esagonale che garantisce la separazione delle frequenze tra celle adiacenti, e non permette frequenze simili entro uno spazio esadecimale, consentendo di poter riutilizzare le frequenze.

Modelli e standard di governance: L'International Telecommunication Union (ITU) è un'agenzia specialistica che svolge un ruolo significativo a livello mondiale per la comunicazione dei dispositivi mobili. Ha una serie di gruppi di lavoro chiamati settori e il settore per gli standard cellulari è l'ITU-R. L'ITU-Radiocommunication (ITU-R) è l'organismo che definisce gli standard e gli obiettivi internazionali per le generazioni di comunicazioni radio e cellulari, con obiettivi di affidabilità e velocità minimi. Due specifiche fondamentali hanno governato la comunicazione negli ultimi anni:

- International Mobile Telecommunication 2000 (IMT-2000): requisiti per un dipositivo 3G;
- International Mobile Telecommunication Advanced (IMT-Advanced): requisiti per un dispositivo 4G.

Third Generation Partnership Project (3GPP) è invece un organismo composto da sette organizzazioni con l'obiettivo di riconoscere gli standard per il Global System for Mobile Communications (GSM) nella creazione delle specifiche per la comunicazione cellulare. In definitiva:

- ITU definisce gli obiettivi e gli standard per un dispositivo 3G, 4G o 5G;
- 3GPP risponde agli obiettivi con tecnologie migliorative per LTE[1];
- ITU conferma che i progressi LTE soddisfano i requisiti per essere etichettati 3G, 4G o 5G.

7.2 5G

Standard di comunicazione basato su IP che utilizza alcune tecnologie 4G LTE, ma presenta nuove funzionalità migliorando la banda, la latenza, la densità e abbassando i costi. Il 5G non è un'evoluzione del 4G. Punta a 3 obiettivi distinti:

- Convergenza tra infrastruttura in fibra e cellulare;
- Cellulari con velocità non teoriche da 1 a 10GBps con copertura mondiale;
- Riduzione significativa dei costi.

Due tipi principali di implementazioni 5G:

[1]LTE: percorso seguito per raggiungere velocità e requisiti ITU-R.

- **Wireless mobile**: utilizza una portante inferiore a 2GHz ottimizzando il raggio di azione, la mobilità e i consumi energetici, basandosi su macrocelle compatibili con LTE in grado di produrre segnali che posso essere trasmessi in qualsiasi situazione. La larghezza di banda di picco è di 100MHz;
- **Wireless fisso**: utilizza frequenze sopra i 6GHz, si basa su una nuova infrastruttura a microcelle ed ha un raggio d'azione limitato, così come la capacità di penetrazione.

La larghezza di banda è 400MHz.

Distribuzione di frequenze: Utilizza onde millimetriche nella banda da 24 a 100GHz, poiché lo spazio millimetrico non è saturo e non è frazionato dai vari organismi, inoltre, sono possibili canali fino a 100MHz nelle frequenze da 30a60GHz. Tuttavia, questa tecnologia ha problemi di attenuazione e di penetrazione.

7.3 LoRaWAN

Tecnologie proprietarie e non sponsorizzate da 3GPP. LoRa è un livello fisico per un protocollo IoT a lungo raggio e bassa potenza, LoRaWAN è un livello MAC. Hanno il vantaggio di utilizzare lo spettro senza licenza abbattendo il costo dell'utilizzo dei dati. Può essere gestito ed utilizzato da chiunque senza necessità di contratti, tuttavia, ha una velocità di trasmissione da 5 a 10 volte inferiore rispetto alle connessioni 3G e LTE.

Sigfox: Protocollo LPWAN a banda stretta che utilizza le bande senza licenza con rigide limitazioni in termini di velocità effettiva ed utilizzo. È destinato ai sistemi che inviano piccole mole di dati poco frequentemente.

Parte IV

Avanzate

Capitolo 8

Architettura Edge e Cloud

8.1 Edge computing

Paradigma di elaborazione dei dati che si basa sulle operazioni di calcolo, memorizzazione dei dati e applicazioni più vicino al punto di origine o di utilizzo dei dati stessi, anziché inviarli a un server o a un data center remoto per l'elaborazione. L'elaborazione avviene in dispositivi locali, noti come "edge devices" o "edge nodes". L'obiettivo principale è ridurre il tempo di risposta tra l'invio dei dati e l'ottenimento dei risultati, migliorando l'efficienza e la velocità delle applicazioni; inoltre, consente di ridurre la quantità di dati che deve essere inviata attraverso la rete verso il cloud. Sfrutta 2 metodi per la comunicazione con internet relativi a sensori e dispositivi perimetrali:

- Sensori e dispositivi hanno un percorso diretto verso il cloud, quindi sono muniti di risorse e accordi sul livello di servizio;
- I dispositivi perimetrali formano aggregazione e cluster attorno a gateway e router per fornire aree di conversioni di protocollo e capacità di elaborazione.

Ai fini della definizione, faremo riferimento ai componenti near-edge e far-edge come segue:

- **Near-edge:** parte dell'infrastruttura tra il cloud e i far-edge; più vicino al cloud, ma più lontano dagli utenti finali;
- **Far-edge:** costituiti da dispositivi in grado di comunicare ed elaborare dati; più lontano dal cloud, ma più vicino agli utenti finali.

Oltre all'ampia definizione di edge computing esiste anche un gergo relativo all'approccio alla progettazione di edge computing:

- **Fog computing:** Architettura di servizi cloud che vanno dai data center ai dispositivi near-edge e far-edge.
- **Multi-access Edge Computing** (MEC): Consente l'esistenza e la distribuzione di applicazioni a bassa latenza, larghezza di banda elevata e in tempo reale ai margini di reti più grandi.
- **Cloudlet:** Data center cloud su piccola scala come un "cloud in a box", è un dispositivo per supportare casi d'uso ad alta intensità di risorse nelle applicazioni di tipo client-server. Simili al MEC, ma non associate ad un'infrastruttura di telecomunicazione.

Per l'edge computer é importante la protezione dell'hardware dalla contaminazione e dall'umidità attraverso custodie elettriche. Esiste una convenzione internazionale chiamata *Ingress Protection Mark (IP)* che ha creato un test per verificare la capacità di un prodotto di preteggere da infiltrazioni di acqua, polveri e corpi estranei. Esistono standard relativi ai test IP.

8.2 Sistemi Operativi

Le scelte sono numerose e meritano attenzioni significative, poiché saranno alla base per eventuali generazioni di soluzioni software distribuite. Esiste come astrazione software e livello di protezione tra

hardware e applicazioni. La modifica di un sistema operativo, spesso, richiede un significativo refactoring di software e driver. Nella maggior parte dei casi gli edge computer hanno risorse limitate e i pacchetti non critici consumano spazio di archiviazione e RAM. In qualunque caso vogliamo che software e sistema siano:

- *Robusti*: in grado di creare, ricevere immagini e rieseguire software dopo la distribuzione;
- *Controllabili*: con un cloud o un servizio centrale che ne gestisce e monitora l'implementazione;
- *Reattivi*: che forniscano segnalazioni sui successi e sui fallimenti.

8.2.1 Windows 10 IoT

Membro della famiglia Windows 10 che offre sicurezza, potenza e gestibilità. Esiste in 2 declinazioni:

- **Core**: esegue una singola applicazione, offre ambiente windows ottimizzato per i dispositivi di dimensioni ridotte con o senza display ed è eseguibile su architetture ARM[1] o x86/64;
- **Enterprise**: versione completa di windows con funzionalità specializzate per dispositivi edge.

8.3 Virtualizzazione

Possiamo distinguere vari tipi di virtualizzazione:

- **Virtualizzazione hardware:** tecnologia che consente di eseguire simultaneamente più macchine virtuali su un singolo server fisico. Un hypervisor, o monitor della macchina virtuale, si trova tra l'hardware fisico e le macchine virtuali, gestendo le risorse hardware e fornendo un ambiente virtuale isolato per l'esecuzione dei sistemi operativi e delle applicazioni delle macchine virtuali e può essere installato direttamente sull'hardware (bare-metal o tipo 1) o eseguito come applicazione (hosted o tipo 2);
- **Paravirtualizzazione:** tecnica in cui il sistema operativo ospite viene modificato per comunicare con l'hypervisor anziché accedere all'hardware fisico, migliorando le prestazioni complessive. Offre vantaggi come prestazioni migliorate, utilizzo efficiente delle risorse e isolamento delle macchine virtuali, ma richiede la modifica del sistema operativo ospite e il supporto specifico dell'hypervisor e dei sistemi operativi ospiti;
- **Container:** tecnologia che consente l'esecuzione di applicazioni in ambienti chiamati "container". A differenza della virtualizzazione hardware tradizionale, dove viene creato un intero sistema operativo virtuale, la virtualizzazione dei container consente di eseguire le applicazioni in modo isolato, condividendo il kernel del sistema operativo host. Si basa su un software chiamato "container engine" o "container runtime" che fornisce l'ambiente per creare, gestire e distribuire i container. Uno dei container engine più popolari è Docker.
- **Docker:** Piattaforma di virtualizzazione dei container che semplifica la creazione, la distribuzione e l'esecuzione di applicazioni all'interno di container, attraverso un'ampia gamma di strumenti e funzionalità che semplificano il ciclo di vita dei container, inclusi i seguenti componenti principali:
  - *Docker Engine:* motore centrale che gestisce la creazione e l'esecuzione dei container;
  - *Docker Image:* pacchetto autonomo che contiene tutto il necessario per eseguire un'applicazione;
  - *Docker Container*: istanza in esecuzione di un'immagine Docker;
  - *Docker Compose:* strumento per la gestione di applicazioni complesse composte da più container;
  - *Docker Registry:* repository centralizzato per l'archiviazione e la condivisione di immagini Docker.

[1] Architettura ARM: famiglia di microprocessori a 32 e 64 bit, utilizzata in molti sistemi embended grazie ai suoi bassi consumi.

8.4 Microsoft Azure IoT Edge

Piattaforma di servizi cloud che estende la funzionalità di IoT fino ai dispositivi edge. Consente di eseguire le applicazioni e i servizi cloud direttamente sui dispositivi edge, riducendo la latenza, ottimizzando l'utilizzo della larghezza di banda di rete e migliorando la sicurezza e la privacy dei dati. Alcune delle sue caratteristiche principali sono:

- Distribuzione di moduli su dispositivi edge;
- Gestione remota dei dispositivi edge;
- Elaborazione dei dati in loco;
- Sicurezza;
- Scalabilità: può essere utilizzata per gestire un gran numero di dispositivi edge distribuiti in modo geografico.

L'hub ha due ruoli:

- **IoT Agent:** gestisce l'immagine del container per ogni modulo in esecuzione sul dispositivo, le credenziali per accedere ai registri dei container privati e le regole sulla creazione e gestione dei moduli;
- **IoT Hub:** gestisce un manifest che indica i moduli qualificati e autenticati che possono essere eseguiti sull'edge device; inoltre, gestisce la comunicazione e funge da proxy verso il cloud.

8.5 Ambient Computing

Si riferisce a un paradigma di calcolo in cui i dispositivi e i servizi informatici sono integrati in modo trasparente nell'ambiente circostante, creando un'esperienza utente immersiva e pervasiva. Invece di focalizzarsi su un singolo dispositivo o una singola interfaccia utente, l'ambient computing mira a fornire un'interazione naturale e senza soluzione di continuità tra le persone, gli oggetti e gli ambienti. Le caratteristiche principali dell'ambient computing includono:

- *Connessione ubiqua:* per creare un ambiente in cui i dispositivi e i servizi sono sempre connessi tra loro e con il cloud, consentendo un accesso costante ai dati e alle risorse, indipendentemente dalla posizione o dal dispositivo utilizzato;
- *Sensori e riconoscimento ambientale:* consentono di monitorare e comprendere l'ambiente circostante, consentendo ai dispositivi di adattarsi in modo intelligente alle preferenze e alle esigenze degli utenti;
- *Interfacce naturali:* interfacce utente intuitive e naturali con l'obiettivo di rendere l'interazione con i dispositivi informatici un'esperienza fluida e integrata nell'ambiente circostante;
- *Automazione e intelligenza artificiale:* automatizzare le attività e fornire servizi personalizzati in base alle preferenze degli utenti e alle informazioni contestuali raccolte dagli ambienti intelligenti.

Si basa inoltre su 4 principi:

- **Invisibile**: i sistemi non attirano l'attenzione su se stessi;
- **Incorporato**: incorporare intelligenza sotto forma di sensori e capacità di elaborazione;
- **Fluido**: rendere trasparenti le più complesse interazioni;
- **Interconnesso**;

8.5.1 Sensori sintetici

Dispositivi posizionati in ambienti in cui sono stati addestrati per apprendere cosa accade sulla base di diversi sensori integrati. Non sono in grado di sfruttare dati video o fotografici poiché formati da dati non strutturati. Gli edge devices li sfruttano in questo modo:

- Acquisiscono i dati del sensore;
- Ripuliscono i dati;
- Normalizzano i dati poiché sensori diversi campionano a frequenze diverse;
- Eseguono modelli di inferenza addestrati sui dati, in tempo reale.

Ottenendo così una classificazione dello stato in cui si trova l'ambiente.

8.6 Protocolli

I protocolli standard sono gli strumenti che legano e incapsulano i dati grezzi da un sensore e li trasformano in qualcosa di significativo e formattato per essere accettato dal cloud. Tra i protocolli abbiamo:

- **TCP e UDP:** Protocolli tipici per il trasporto dei dati su internet. TCP è stabile, affidabile e orientato alla connessione, ma complesso nell'implementazione. UDP, al contrario, non è stabile, né affidabile e neanche orientato alla connessione, ma è molto più semplice da implementare;
- **MQTT;**

Message-Oriented Middleware (MOM) MOM è un'infrastruttura software o hardware che supporta l'invio e la ricezione di messaggi tra sistemi distribuiti. La comunicazione tra due dispositivi avviene utilizzando code di messaggi distribuite attraverso il paradigma del produttore-consumatore. Alcune implementazioni sfruttano un broker che funge da intermediario attraverso paradigmi di sottoscrizione e pubblicazione. Le code sono tali da mantenere i dati anche in caso di guasti.

RESTful L'alternativa all'implementazione MOM è RESTful. La comunicazione avviene attraverso il modello client-server. Il server possiede lo stato di una risorsa che viene trasferito al client attraverso messaggi. Le implementazioni sfruttano metodi HTML per inserire le richieste nell' Universal Resource Identifier (URI). Gode della maggior parte dei servizi offerti da HTML. L'URI viene utilizzato come identificatore per il traffico dati basato sul web; il più importante è l'Universal Resource Locator (URL) e può essere suddiviso in diverse componenti da usare a vari livelli dello stack di rete. Ad esempio "http://www.iotforarchitets.net:8080/iot/?id="temperatura"" contiene:

```
Schema: http://;
Autorita': www.iotforarchitets.net;
Porta: 8080 ;
Percorso: /iot;
Domanda: ?id:"temperatura";
```

8.6.1 Message Queuing Telemetry Transport (MQTT)

Concepito per affrontare i problemi nei sistemi distribuiti indipendenti e non concorrenti, per aiutarli a comunicare in modo sicuro. Glio obiettivi sono:

- Semplice da implementare;
- In grado di gestire la Quality of Service (QoS);
- Leggero ed efficiente in termini di larghezza di banda;
- Indipendente dai dati;
- Costante consapevolezza della sessione;
- Affrontare i problemi di sicurezza.

È un protocollo di messaggistica, pubblicazione e sottoscrizione, estremamente semplice e leggero, progettato per dispositivi vincolati e reti a bassa larghezza di banda, alta latenza o inaffidabili, attraverso la riduzione della larghezza di banda della rete e dei requisiti di risorse del dispositivo, tentando di garantire la consegna (grazie al fatto che è basato su TCP).
Nonostante il nome, non sono previste code di messaggio inerenti al protocollo, sebbene sia possibile farlo. Prevede la presenza di sottoscrizioni e pubblicazioni gestite attraverso dei broker che conservano i messaggi a tempo indeterminato, attraverso l'uso di flag.

8.6.1.1 MQTT-SN

Progettato principalmente per le reti di sensori, mantiene la filosofia di MQTT, ma per WPAN. Non è basato su protocollo IP e può essere utilizzato o su collegamento seriale, o con protocollo UDP. Ci sono quattro componenti fondamentali:

- **Gateway**: converte i dati da MQTT-SN a MQTT e viceversa;
- **Forwarder**: nodi tra client e gateway, reincapsulano i frame in nuovi frame invariati reinoltrandoli, fino a quando non arrivano a destinazione;
- **Client**: si comportano allo stesso modo di MQTT, sono in grado di sottoscrivere e pubblicare dati;
- **Broker**: si comportano allo stesso modo di MQTT.

Capitolo 9

Vulnerabilità e Protezione dei Sistemi IoT

9.1 Tipologie di Attacchi alle Reti

- *Attacco di amplificazione:* Ingrandisce la larghezza di banda utilizzata dalla vittima utilizzando un servizio legittimo come NTP o DNS. NTP può aumentare di 556 volte, DNS di 179.
- *Spoofing ARP:* Invia un messaggio ARP falsificato che produce una falsa associazione tra l'indirizzo MAC dell'attaccante e l'IP di un sistema legittimo.
- *Scansioni banner:* Tecnica utilizzata per fare l'inventario dei sistemi su una rete che può essere utilizzata da un utente malintenzionato per ottenere informazioni su un potenziale bersaglio, eseguendo richieste HTTP e ispezionando le informazioni restituite dal sistema.
- *Distributed Denial of Service (DDoS):* Tentativo di interrompere o un servizio online sovraccaricandolo da più fonti.
- *Botnet:* Dispositivi connessi a internet infettati e compromessi da malware che operano collettivamente mediante un controllo comune, utilizzati per effettuare attacchi DDoS.
- *Forza bruta:* Metodo per tentativi ed errori per accedere a un sistema o aggirare la crittografia.
- *Overflow del buffer:* Sfrutta un bug o un difetto si un software per sovraccaricare un blocco di memoria con più dati di quelli allocati, sovrascrivendo i dati adiacenti al blocco stesso. Questa vulnerabilità può essere sfruttata per inserire codice dannoso in quell'area e costringere la macchina ad eseguirlo.
- *Slitte NOP:* Sequenza di istruzioni di assemblaggio NOP iniettate per far scorrere il puntatore di istruzioni di una CPU nell'area di codice dannoso, fa parte di un attacco di overflow.
- *Exploit RCE:* Esecuzione di codice arbitrario in modalità remota. Si presenta sotto forma di attacco di overflow del buffer su HTTP o altri protocolli di rete.
- *Attacco di analisi della potenza correlata:* Consente di scoprire chiavi di crittografia archiviate in un dispositivo, attraverso quattro passaggi:
  - Esamina il consumo energetico di un target e lo registra per ogni fase del processo di crittografia.
  - Forza la destinazione a crittografare diversi oggetti di testo in chiaro;
  - Attacca piccole parti della chiave considerando ogni possibile combinazione;
  - Mette insieme le migliori sottochiavi per ottenere la chiave completa.
- *Attacco a dizionario:* Metodo per accedere a un sistema di rete inserendo parole da un file dizionario (grandi elenchi di testi).

- *Fuzzing:* Invio di dati non corretti o non standard per osservare il comportamento dei dispositivi esposti a vulnerabilità.
- *Attacco Man In The Middle (MITM):* Pone un dispositivo in mezzo ad un flusso di comunicazione tra due parti ignare. Il dispositivo ascolta, filtra, si appropria delle informazioni dal trasmettitore e ritrasmette le informazioni selezionate al ricevitore.
- *Return to libc:* Inizia con un buffer overflow in cui viene iniettato codice per passare a librerie comunemente utilizzate nello spazio di memoria dei processi, nel tentativo di chiamare le routine di sistema.
- *Rootkit:* Software utilizzato per rendere non rilevabili i payload di altri software attraverso tecniche come gli overflow del buffer.
- *Attacco side-channel:* Utilizzato per ottenere informazioni su una vittima, osservando gli effetti secondari del sistema fisico, anziché trovando exploit.
- *Ingegneria sociale:* Manipolazione psicologica ed inganno personale per ottenere informazioni private.
- *Spoofing:* Il dispositivo dannoso impersona un altro dispositivo o utente sulla rete.
- *SQL injection:* Effettuato con l'intento di distruggere il contenuto di un database che utilizza istruzioni SQL.
- *SYN flood:* Falsificazione di pacchetti TCP:SYN, così da far creare connessioni semiaperte a molti indirizzi inesistenti esaurendo le risorse dell'host.
- *XSS:* Vulnerabilità nelle applicazioni web sfruttata per inserire script lato client.
- *Exploit zero day:* Vulnerabilità sconosciute prima di quel giorno.

9.2 Tecniche per la Difesa Informatica

- *Address Space Layout Randomization (ASLR):* Protegge la memoria e contrasta gli overflow del buffer mediante randomizzazione del punto in cui un eseguibile viene caricato in memoria.
- *Buco nero:* Dopo aver rilevato un attacco DDoS, stabilisce percorsi per forzare i dati non autorizzati ad un endpoint inesistente.
- *Prevenzione esecuzione dati (DEP):* Contrassegno di aree come eseguibili, così da limitare la possibilità di iniettare ed eseguire codice dannoso, sollevando eccezioni o errori di sistema.
- *Deep Packet Inspection (DPI):* Metodo per ispezionare ogni pacchetto isolando quelli considerati dannosi.
- *Firewall:* Costrutto di sicurezza che concede o rifiuta l'accesso di rete ai flussi di pacchetti controllandolo e gestendolo attraverso elenchi di controllo di accesso.
- *Honeypot:* Appaiono come siti web legittimi o nodi accessibili, ma in realtà sono isolati e monitorati.
- *Sistema di rilevamento delle intrusioni (IDS):* Costrutto di rete per rilevare le minacce attraverso l'analisi fuori banda del flusso di pacchetti.
- *Sistema di prevenzione delle intrusioni (IPS):* Blocca le minacce a una rete tramite una vera analisi in linea e il rilevamento statistico o delle firme delle minacce.
- *Milkers:* Strumento difensivo che emula un dispositivo botnet infetto e si collega al suo host malevolo consentendo di comprendere e prelevare i comandi del malware inviati alla botnet controllata.
- *Root of Trust (RoT):* Avvia l'esecuzione su un dispositivo di avvio a freddo da una fonte di memoria attendibile immutabile (come la ROM); se il software di avvio/BIOS anticipato può essere modificato senza controllo, non esiste RoT.

- *Chiave pubblica:* Chiave generata con una chiave privata ed è accessibile a entità esterne; può essere utilizzata per decrittografare gli hash.
- *Infrastruttura a chiave pubblica (PKI):* Definizione di gerarchie di verificatori per garantire l'origine di una chiave pubblica.
- *Chiave privata:* Chiave generata con una chiave pubblica, mai rilasciata esternamente e archiviata in modo sicuro; utilizzata per crittografare gli hash.
- *Avvio sicuro:* Serie di passaggi di avvio per un dispositivo che si avvia a un RoT e procede attraverso il caricamento del sistema operativo e dell'applicazione in cui ogni firma del componente viene verificata come autentica tramite chiavi pubbliche caricate nelle precedenti fasi di avvio attendibile.
- *Stack canary:* Protegge lo spazio dello stack di elaborazione dai sovraccarichi dello stack e impedisce l'esecuzione di codice da uno stack.
- *Ambiente di esecuzione attendibile (TEE):* Area sicura di un processore che garantisce la protezione del codice e dei dati che risiedono all'interno di questa zona; solitamente è un ambiente di esecuzione sul core del processore principale in cui la gestione della chiave privata viene eseguita con un livello di sicurezza più elevato rispetto alla maggior parte del codice.

9.3 Attacchi Famosi

Tre attacchi verso sistemi IoT:

- **Mirai**: l'attacco DoS più dannoso della storia, generato da dispositivi IoT non sicuri in aree remote;
- **Stuxnet**: arma informatica di uno stato nazionale che prende di mira i dispositivi IoT SCADA industriali che controllano le centrifughe di arricchimento dell'uranio e causano danni sostanziali e irreversibili al programma nucleare iraniano;
- **Reazione a catena**: metodo di ricerca per sfruttare il PAN utilizzando nient'altro che una lampadina, senza bisogno di Internet.

9.3.1 MIRAI

Nome del malware che ha infettato i dispositivi IoT Linux nell'agosto del 2016. L'attacco è arrivato sotto forma di una botnet che ha generato una massiccia tempesta DDoS. Gli obiettivi includevano Krebs on Security, un popolare blog sulla sicurezza di Internet; Dyn, un provider DNS ampiamente utilizzato per Internet e Lonestar cell, un operatore di telecomunicazioni in Liberia, siti politici italiani, server Minecraft in Brasile e siti di aste russi. Il DDoS su Dyn ha avuto effetti secondari su altri provider che utilizzavano i loro servizi, come i server Sony Playstation, Amazon, GitHub, Netflix, PayPal,Reddit e Twitter. Sono stati infettati complessivamente 600.000 dispositivi IoT. Scansione delle vittime:

- Rapida scansione asincrona utilizzando i pacchetti TCP:SYN per sondare indirizzi IPv4 casuali;
- Ha cercato specificamente la porta SSH/Telnet TCP 23 e la porta 2323;
- Se indirizzo IP e porta risultavano raggiungibili, venivano registrati ed utilizzati dalla fase due.

Includeva una lista nera di indirizzi da evitare composta da 3,4 milioni di indirizzi IP appartenenti al servizio postale degli Stati Uniti, Hewlett-Packard, GE e il Dipartimento della Difesa degli Stati Uniti. Mirai era in grado di scansionare a velocità di circa 250 byte al secondo; il motivo principale di tale bassa velocità è che i dispositivi IoT in genere sono molto più limitati nella potenza di elaborazione rispetto ai dispositivi desktop e mobili.

Telnet a forza bruta: Mirai ha tentato di stabilire una sessione Telnet con ogni vittima individuata in fase 1, inviando casualmente 10 coppie di nome utente e password utilizzando un attacco dizionario di 62 coppie; se l'accesso riusciva, registrava l'host su un server C2 centrale.

Infect: Il server MIRAI provvedeva ad inviare un loader[1] alla potenziale vittima. Cercava poi altri processi concorrenti utilizzanti la porta 22 o 23 e ne interrompeva l'esecuzione insieme ad altri malware che potrebbero essere stati già presenti sul dispositivo. Il file binario del loader veniva poi eliminato ed il nome del processo veniva offuscato. Il bot rimaneva inattivo fino a quando non riceveva il comando di attacco. Il danno si è limitato ad interruzioni di servizio generando 623 Gbps di traffico.

9.3.2 STUXNET

È stata la prima arma informatica documentata nota rilasciata per danneggiare i beni dell'Iran. Si trattava di un worm che veniva rilasciato per danneggiare i controllori logici programmabili (PLC) Siemens basati su SCADA e utilizzava un rootkit per modificare la velocità di rotazione dei motori sotto il controllo diretto del PLC; solo i dispositivi collegati a PLC, poiché generalmente utilizzati per pompe e centrifughe a gas per l'arricchimento di uranio. Il processo di infezione ha seguito questi passaggi:

- **Infezione iniziale:** il worm è iniziato infettando un computer Windows host sfruttando le vulnerabilità rilevate in precedenti attacchi di virus. Ha utilizzato quattro exploit zero-day contemporaneamente (un livello di sofisticazione senza precedenti). Gli exploit hanno utilizzato un attacco rootkit utilizzando codice in modalità utente e modalità kernel e hanno installato un driver di dispositivo rubato ma correttamente firmato e certificato da Realtek. Questo driver firmato in modalità kernel era necessario per nascondere Stuxnet ai pacchetti antivirus diffidenti;
- **Attacco e diffusione di Windows:** il worm ha iniziato a cercare nel sistema Windows i file tipici di un controller SCADA Siemens; se trovava il software di controllo, tentava di accedere a Internet tramite un C2 utilizzando URL non corretti per scaricare sue versioni più recenti. Cercava poi ulteriormente nel filesystem per individuare un file chiamato "s7otbdx.dll", che fungeva da libreria di comunicazione critica tra la macchina Windows e il PLC, per agire come un attaccante manin-the-middle. Il virus ha iniziato la sua attività registrando il normale funzionamento delle centrifughe;
- **Distruzione:** ha riprodotto i dati preregistrati ai sistemi SCADA, infliggendo il suo danno manipolando i PLC con due diversi attacchi coordinati per danneggiare l'intera schiera della struttura iraniana.

Il danno ai rotori della centrifuga si è verificato lentamente nel tempo, con incrementi di 15 o 50 minuti separati da 27 giorni di normale funzionamento. Ciò ha prodotto uranio arricchito in modo improprio, perni dei rotori delle centrifughe incrinati o addirittura distrutti. Si ritiene che oltre 1.000 centrifughe di arricchimento dell'uranio siano state paralizzate e danneggiate da questo attacco al principale impianto di arricchimento iraniano.

9.3.3 Reazione a catena

È uno studio accademico che mostra una nuova generazione di attacchi informatici incentrati sulle reti mesh PAN che possono essere eseguiti senza alcun collegamento a Internet. Mostra quanto possono essere vulnerabili i sensori e i sistemi di controllo IoT remoti. Il vettore di attacco è costituito dalle lampadine Philips Hue che possono essere controllate da Internet e dalle app per smartphone. L'exploit può essere esteso agli attacchi delle smart city e avviato semplicemente inserendo una singola lampada intelligente infetta. Le luci Philips Hue utilizzano il protocollo Zigbee per stabilire una mesh. I sistemi di illuminazione Zigbee rientrano in un programma chiamato Zigbee Light Link (ZLL). I messaggi ZLL non sono crittografati o firmati ma la crittografia viene utilizzata per proteggerelechiavi scambiate se viene aggiunta una lampada alla rete mesh. Questa chiave è trapelata all'esterno dell'alleanza. ZLL impone che le lampade che si uniscono alla rete debbano essere molto vicine all'iniziator per impedire che ci si possa impossessare delle luci del vicino. Zigbee offre anche un metodo di riprogrammazione over-the-air (OTA) e i pacchetti del firmware sono crittografati e firmati. Piano di attacco in quattro fasi:

- Rompe la crittografia e la firma del pacchetto firmware OTA;
- Distribuisce un aggiornamento del firmware malevolo su una singola lampadina usando la crittografia rotta e le chiavi di firma;

[1] Loader:programma responsabile dell'identificazione del sistema operativo e dell'installazione di malware specifico per quel dispositivo.

- La lampadina compromessa si unisce alla rete in base alla chiave principale rubata e sfrutta la sicurezza di prossimità attraverso un difetto zero-day trovato nella parte Atmel At Mega comunemente utilizzata;
- Dopo essersi unita con successo a una rete Zigbee, invia il suo carico utile alle luci vicine, infettandole rapidamente. Il processo si espande e infetta interi sistemi di illuminazione cittadini.

Zigbee utilizza la crittografia AES-CCM per crittografare gli aggiornamenti del firmware OTA. Per violare la crittografia del firmware, gli aggressori hanno utilizzato l'analisi della potenza di correlazione (CPA) e l'analisi della potenza differenziale (DPA). CPA e DPA sono forme di attacco sofisticate, in cui un dispositivo come l'hardware del controller della lampadina viene posizionato su un banco e viene misurata la potenza che consuma; è possibile misurare la potenza dinamica utilizzata da una CPU che esegue un'istruzione o sposta dati. Metodo chiamato analisi della potenza semplice (SPA), con il quale però risulta ancora molto difficile decifrare la chiave. CPA e DPA estendono le capacità oltre SPA utilizzando una correlazione statistica. I ricercatori hanno corrotto il sistema di illuminazione Philips Hue come segue:

- Hanno utilizzato il CPA per decifrare l'AES-CBC;
- Hanno usato DPA per decifrare la modalità contatore AES-CTR per rompere la crittografia del bundle del firmware ed hanno trovato 10 posizioni che l'AES-CTR sembrava eseguire, il che ha esposto 10 possibilità;
- Si sono quindi concentrati sulla violazione della protezione di prossimità Zigbee per l'adesione a una rete.

L'exploit zero-day è stato il risultato trovato ispezionando il codice sorgente di Atmel per il bootloader sul SOC. Dopo aver esaminato il codice, hanno scoperto che il controllo di prossimità era valido quando si avviava una richiesta di scansione in Zigbee; se iniziavano con un altro messaggio, il controllo di prossimità veniva ignorato. Ciò ha permesso loro di unirsi a qualsiasi rete

Queste dispense sono state preparate con LaTeX, esse costituiscono soltanto un ausilio per lo studente , quindi non sono in nessun modo sostitutive dei testi consigliati. Il PDF è dotato di hyperlinking quindi è possibile cliccare sui nomi delle sezioni nell'indice per spostarsi tra le pagine, allo stesso modo, per tornare all'indice è sufficiente cliccare sul numero della pagina.