POLITECNICO DI MILANO





Protocolli di comunicazione Machine-to-Machine: verso il cellular IoT

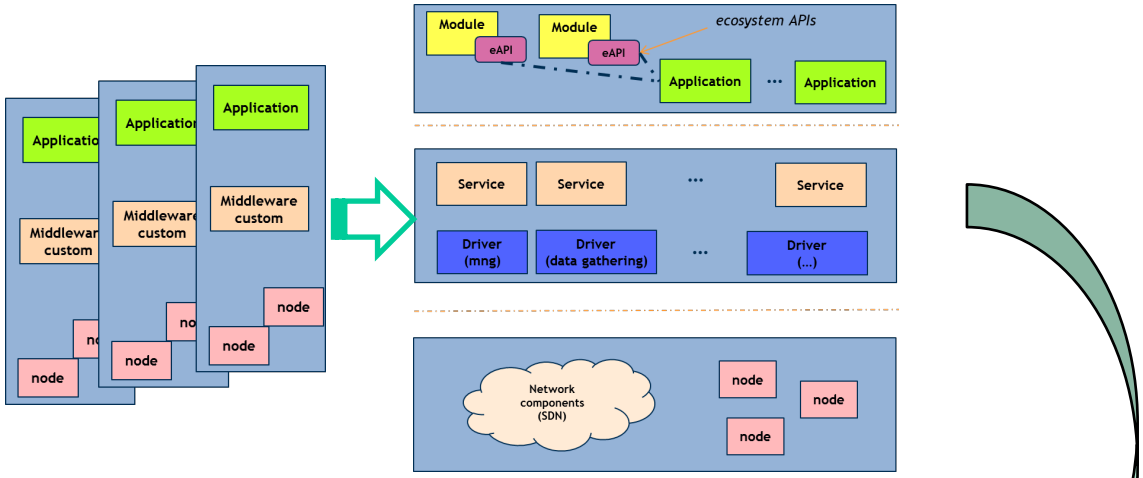
Antonio Capone, Giacomo Verticale

Dipartimento di Elettronica, Informazione e Bioingegneria

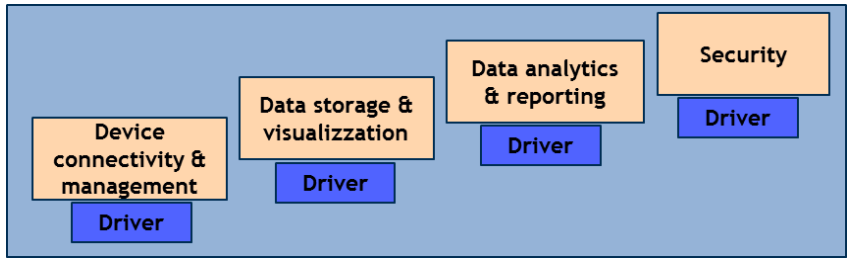
Politecnico di Milano

Le piattaforme per l'IoT
L'evoluzione della architettura di riferimento

L'approccio *verticale* classico evolve verso una logica *orizzontale*, multi-applicativa



Il livello intermedio, di mediazione, diventa una collezione di servizi, spesso erogabili in logica cloud → piattaforme IoT

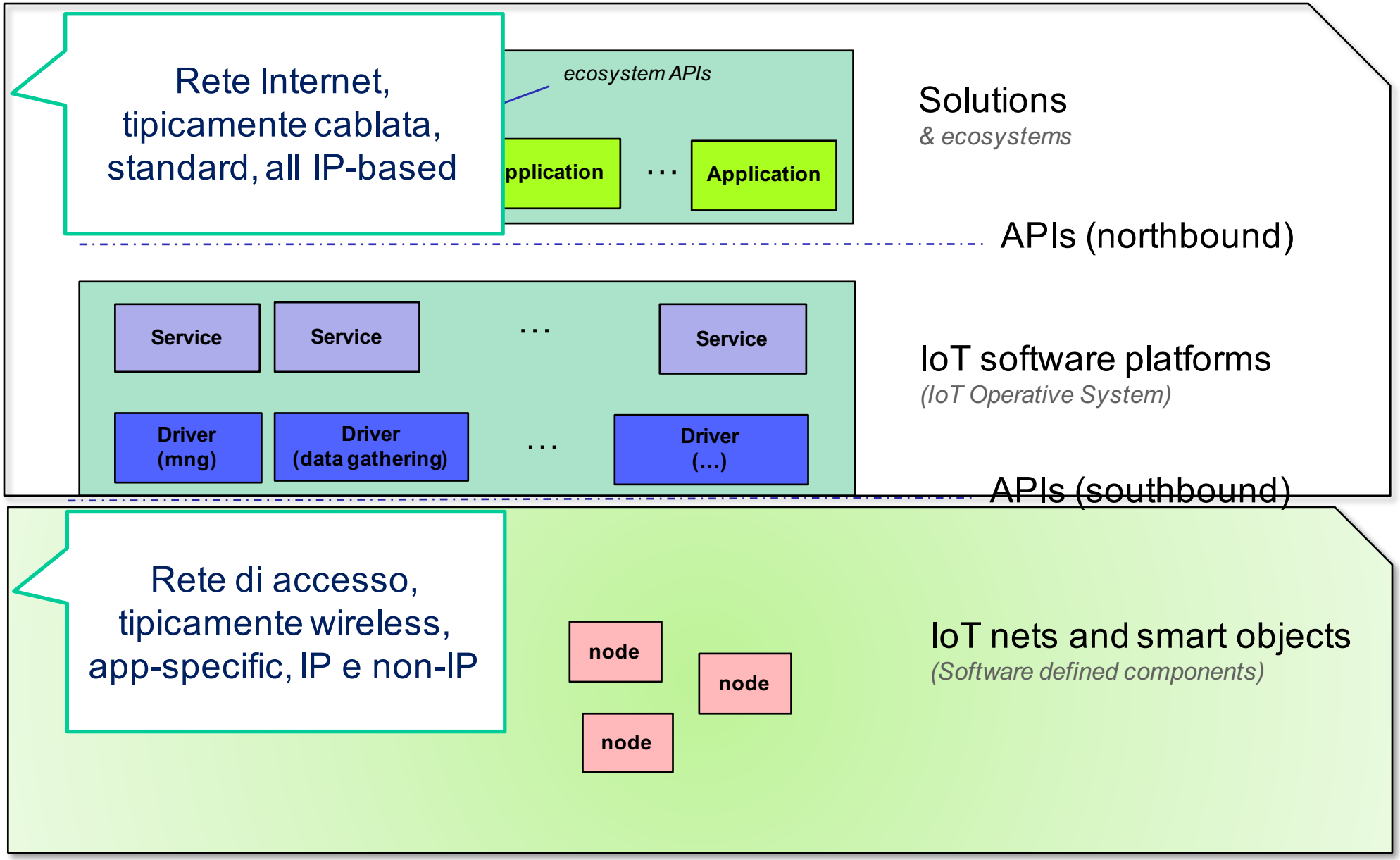


I servizi si stanno stratificando, diventando componibili, all'interno di una stessa piattaforma o tra piattaforme diverse

Tutto si traduce in costi di sviluppo e time-to-market più contenuti → vantaggio competitivo

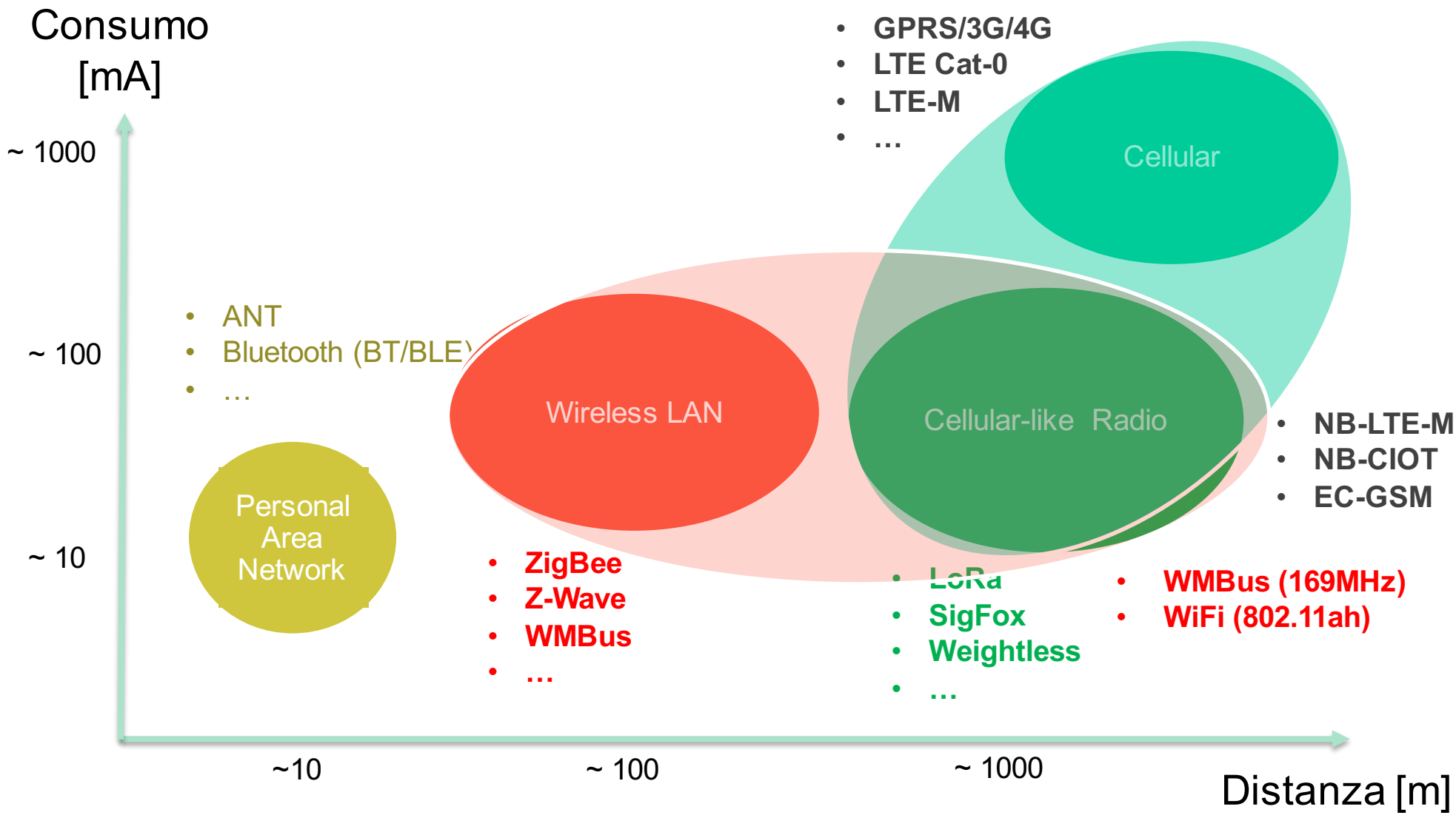
Architettura IoT orizzontale

Elementi della comunicazione



Protocolli per la connettività

Copertura vs Consumo



Protocolli cellular-like (LPWAN)
Principali caratteristiche

Autonomia energetica

- Durata batterie >5 anni
- Dipende da molti fattori (potenza, # messaggi, banda, Tx/Rx, capacità batteria, ecc.)

Spettro non licenziato

- Banda ISM senza licenza
- Forti limitazioni d'uso e duty cycle
- Frequenze diverse da regione a regione

Banda (molto) stretta

- Distanze di com. elevate
- Consumo ridotto
- Velocità di Tx molto bassa
- Alta scalabilità (# nodi gestibili)

SIGFOX

WEIGHTLESS™

LoRa™

INGENU

Protocolli cellular-like vs cellulari

Costi dell'infrastruttura

Costi contenuti

- Le reti LPWAN vantano rapporti di concentrazione e distanze di trasmissione molto elevate
- Es. su una città <10 Base Station Lora/Sigfox vs >100 cellular

Costi operativi

- La complessità molto ridotta delle reti LPWAN si traduce in costi operativi ridotti
- Mancanza di licenze per accesso allo spettro

Garanzie/SLA

Meno garanzie

- L'uso delle bande ISM, license-free, comporta l'impossibilità di fornire alcuna garanzia o accordi SLA per servizi mission-critical (forte limitazione)
- Senza alcun controllo, la proliferazione dell'uso di questi protocolli porterà a una saturazione della banda disponibile nel futuro

Protocolli cellulari

Ma i protocolli cellulari sono in “veloce” evoluzione

- Sperimentazione di nuovi protocolli cellulari
- Due approcci diversi:
  - In ottica evolutiva (senza cambiare la rete esistente): **LTE Cat M** e **NB-LTE**
  - In ottica clean-slate: **NB-CIoT (ed altri)**

LTE cat M
Tutti produttori

NB-LTE

Nokia Networks

ERICSSON

intel

NB-CIoT

HUAWEI

Evoluzione tecnologie cellulari per M2M

3GPP Release	8	8	12	12/13	12		
	Cat-4	**Cat-1**	**Cat-0**	**LTE-M**	**NB LTE-M**	**EC-GSM**	**C-IOT**
Spettro (MHz)	700-900					800-900	700-900
Ampiezza Canale	20 MHz			1.4 MHz	200 kHz		5 kHz (UL) 3.75 kHz (DL)
TX rate (DL)	150 Mbit/s	10 Mbit/s	1 Mbit/s	200 kbit/s	200 kbit/s	300 kbit/s	200 kbit/s
TX rate (UL)	50 Mbit/s	5 Mbit/s	1 Mbit/s	200 kbit/s	144 kbit/s	<10 kbit/s	48 kbit/s
Duplexing	full		half				
TX power UL (dBm)	23			20	23	23-33	<23
Costo (rispetto a Cat-1)	1.4	1	0.4	0.2	<0.15		
Disponibilità	disponibile			2016			

Rischi di sicurezza nella comunicazione M2M

Privacy

- accesso a dati personali aggiuntivi che esulano dallo scopo del servizio
- esempio: Smart Meter Discovergy (Germania) violato per ottenere misure con periodo 2 s, sufficienti per identificare programmi TV

Frodi

- deployment in ambiente ostile
- esempio: furto di SIM da semafori (Sud Africa)

Esposizione di infrastrutture critiche

- possono attrarre attaccanti con maggiori budget. Possibili danni alle infrastrutture
- esempio: azionamento di pompe idriche da remoto (Olanda)
- esempio: controllo remoto Jeep (USA)

Sicurezza: considerazioni

Gli attacchi raramente sfruttano vulnerabilità della rete di comunicazione, ma più spesso vulnerabilità nel progetto software o hardware

La disponibilità di un canale accessibile tramite una rete di comunicazione consente all'operatore della rete di supportare gli utenti M2M nel rendere più sicuri i dispositivi:

- monitorando le connessioni
- sfruttando le attuali catene di autenticazione e sicurezza (eSIM)
- sfruttando i canali over-the-air per la gestione remota e il deployment degli aggiornamenti di sicurezza