Sicurezza dei sistemi e delle reti[1]

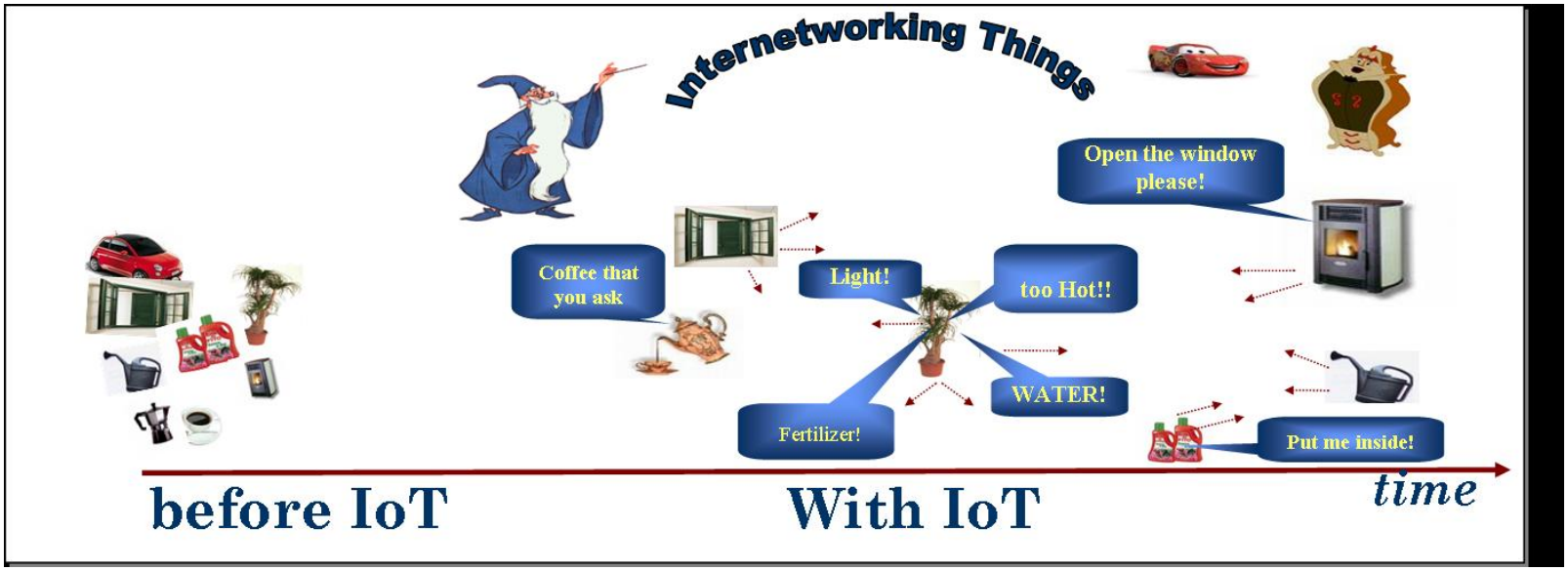
Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2014/15

Lezione XIX: Wireless

Internet of Things



- Ogni oggetto dell'ambiente in cui siamo immersi potrebbe diventare un nodo intelligente di una rete di sensori.
- La realizzazione di servizi richiede lo scambio di dati e computazioni.

Problemi di sicurezza

- Le interazioni sono spesso decentralizzate
- Potenza limitata: alimentazione, capacità di calcolo, di memorizzazione, di primitive crittografiche
- Comunicazioni wireless
- malicious displacement, impersonation, and tampering

Secure data aggregation

Perché la crittografia tradizionale non è sufficiente

hop-by-hop, ma in ogni nodo è in chiaro

end-to-end, ma serve qualche segreto condiviso o crittografia asimmetrica (generalmente considerata irrealizzabile in WSN)

Castelluccia *et al.* [TOSN 2009]:

- end-to-end stream cipher: $C \oplus K = E \Rightarrow E \oplus K = C$
- usando *modular addition* $(+^m)$ invece dello *xor*: $C +^m K = E \Rightarrow (E_1 + E_2) = (C_1 + C_2) +^m K$
- In questa maniera gli aggregatori non necessitano la chiave

La locazione dei nodi

Non è sempre nota a priori.

- nodi sparsi casualmente, mobili, ecc.
- in questo caso non è un dato topologico di sistema, o semplicemente *trasmesso*
- viene *calcolato* da una *base station* con le informazioni ricevuto da nodi collaboranti

Un protocollo di localizzazione

Multilateration

- Un certo numero di landmark o ancore v_i vengono usate per la verifica
- I landmark scambiano beacon con i nodi da localizzare e trasmetto informazioni sui range

Several attacks known:

Node displacement

Wormholes (fabricated communication links)

Distance enlargement (con nodi fake)

Dissemination of false position and distance information (con nodi compromessi)

Localizzazione

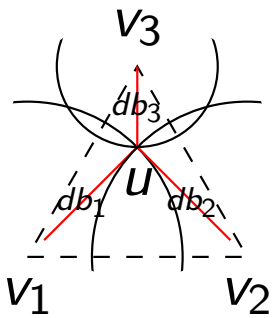
- Ogni verificatore calcola dei distance bound db_i rispetto a un nodo sconosciuto u
- Un attaccante che controlla un solo nodo può *ritardare* un beacon, ma non accelerarlo: quindi può solo apparire piú *lontano*, non piú vicino.

Secure localization

Čapkun *et al.* [IEEE JSACOMM 2006]
Servono almeno 3 verificatori di cui la base station (sink) si fida.

1. Determina u' in modo che minimizzi la somma dei delta fra i db_i e la distanza $u' - v_i$
2. Se la somma è maggiore dell'errore atteso $\rightsquigarrow$malicious
3. Altrimenti:

Se u' è contenuto in almeno un triangolo di verificatori: l'informazione è sicura, perché qualsiasi falsificazione deve accorciare un db_i



Output

Alla fine la base station può marcare le posizioni come

Robust almeno un triangolo di verificatori "certifica" il dato.

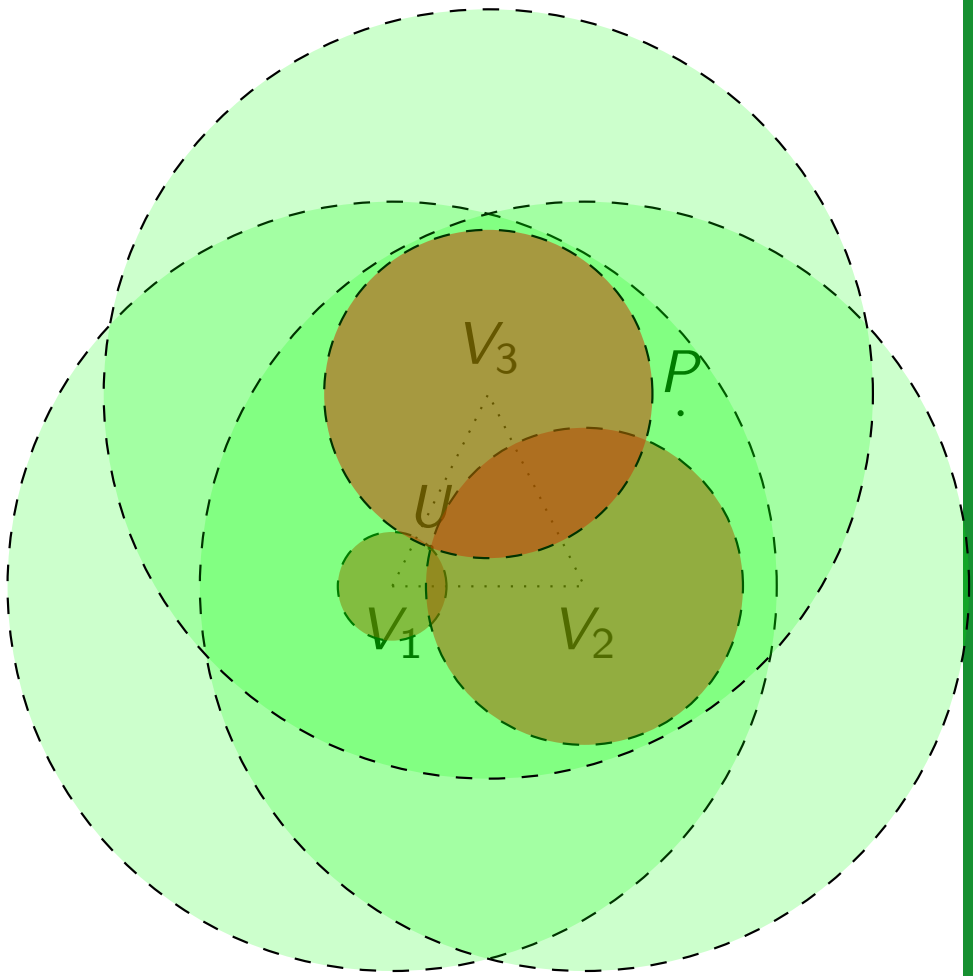
Malicious l'errore è troppo elevato perché sia casuale

Unknown

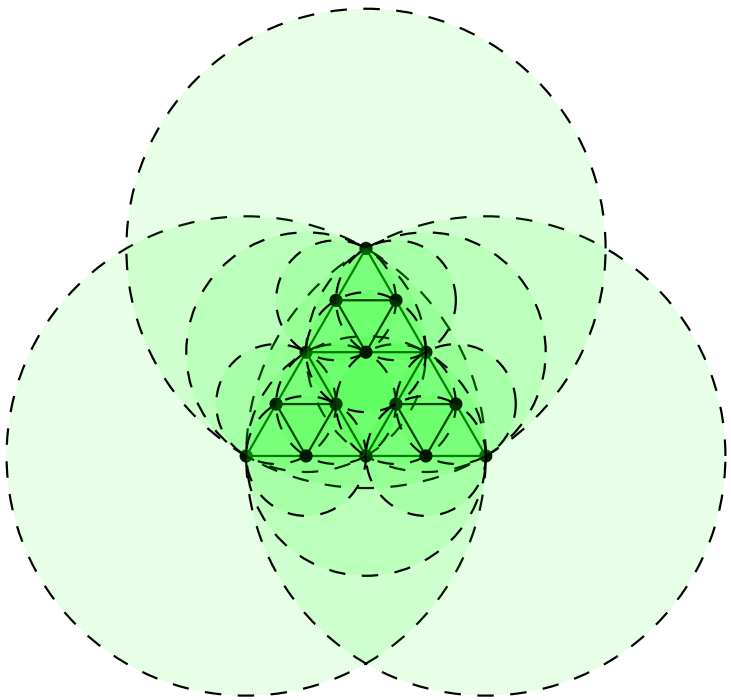
Esempio

L'attaccante può decidere dove piazzarsi (U) e quale posizione falsificare (P)

- Senza "restringere" distanze



- Power range green
- Distance bound red



# ver.	max. deception
3	$0.2516\ R$
6	$0.1258\ R$
15	$0.0629\ R$
42	$0.02145\ R$
123	$0.015725\ R$
366	$7.8625 \cdot 10^{-3} R$