ttp | The Technology Partnership

How to choose an IoT RAN

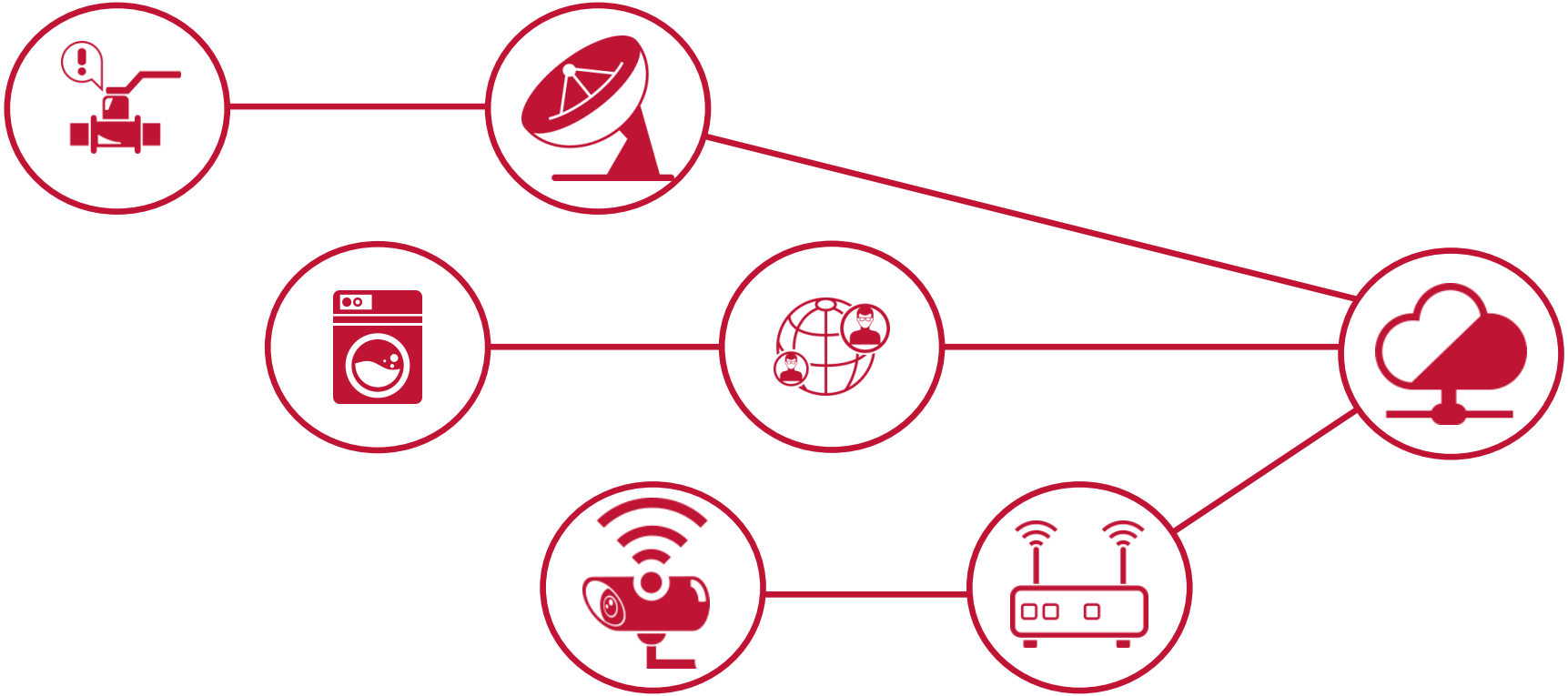
Surely your thing doesn't need a wire!

Joe Milbourn

The Technology Partnership plc
+44 1763 262626

www.ttp.com

radio access networks



examples of things

remote monitoring

low bandwidth, worldwide connections

low power consumption

home or industrial sensing & control

low bandwidth local/regional connections

low power consumption

connected cameras

high bandwidth local connections

lots* of processing power

real things

ttp | The Technology Partnership

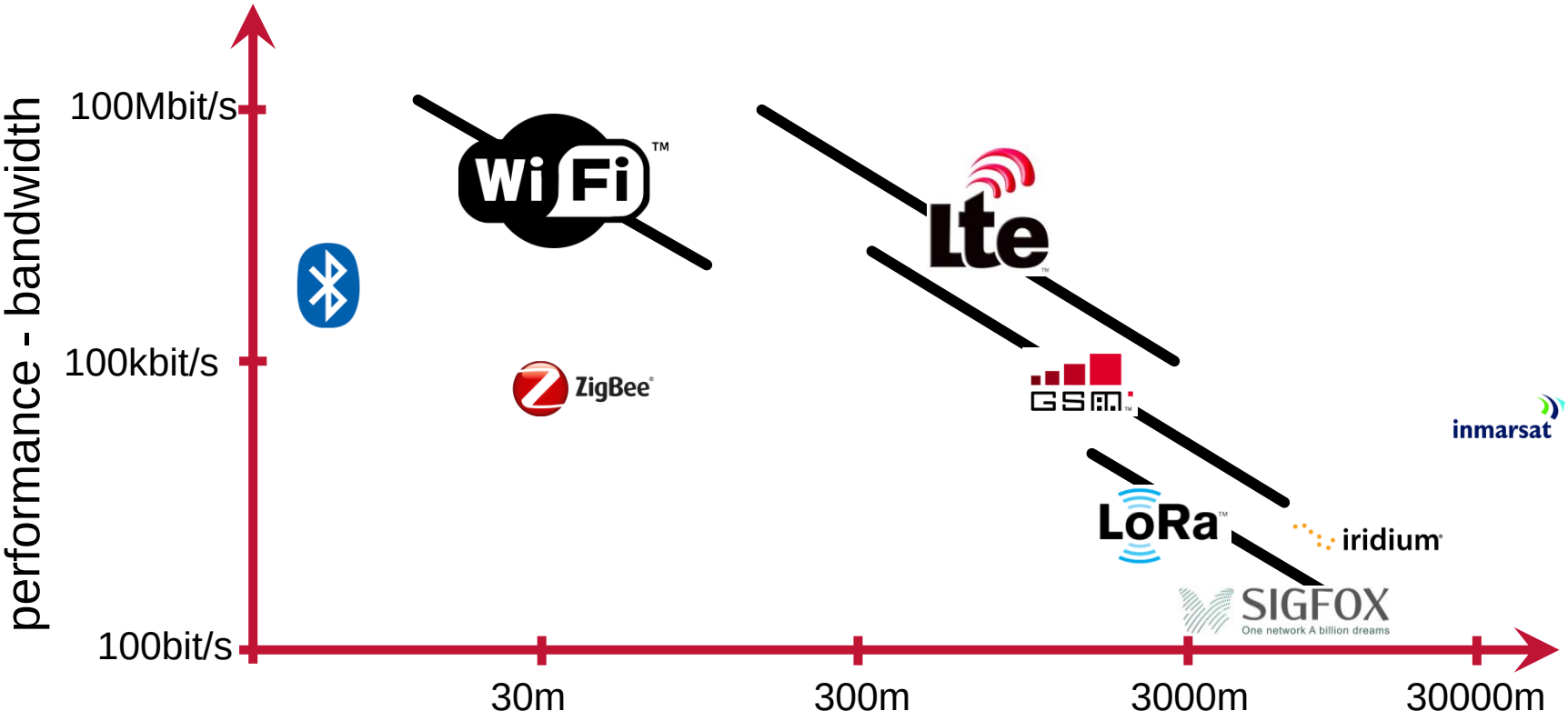
conflicting requirements

- low normal data rates, and uplink only
  - but might need key exch. or fw upgrade

- long range and low power
  - range → energy per bit → battery size or data rate

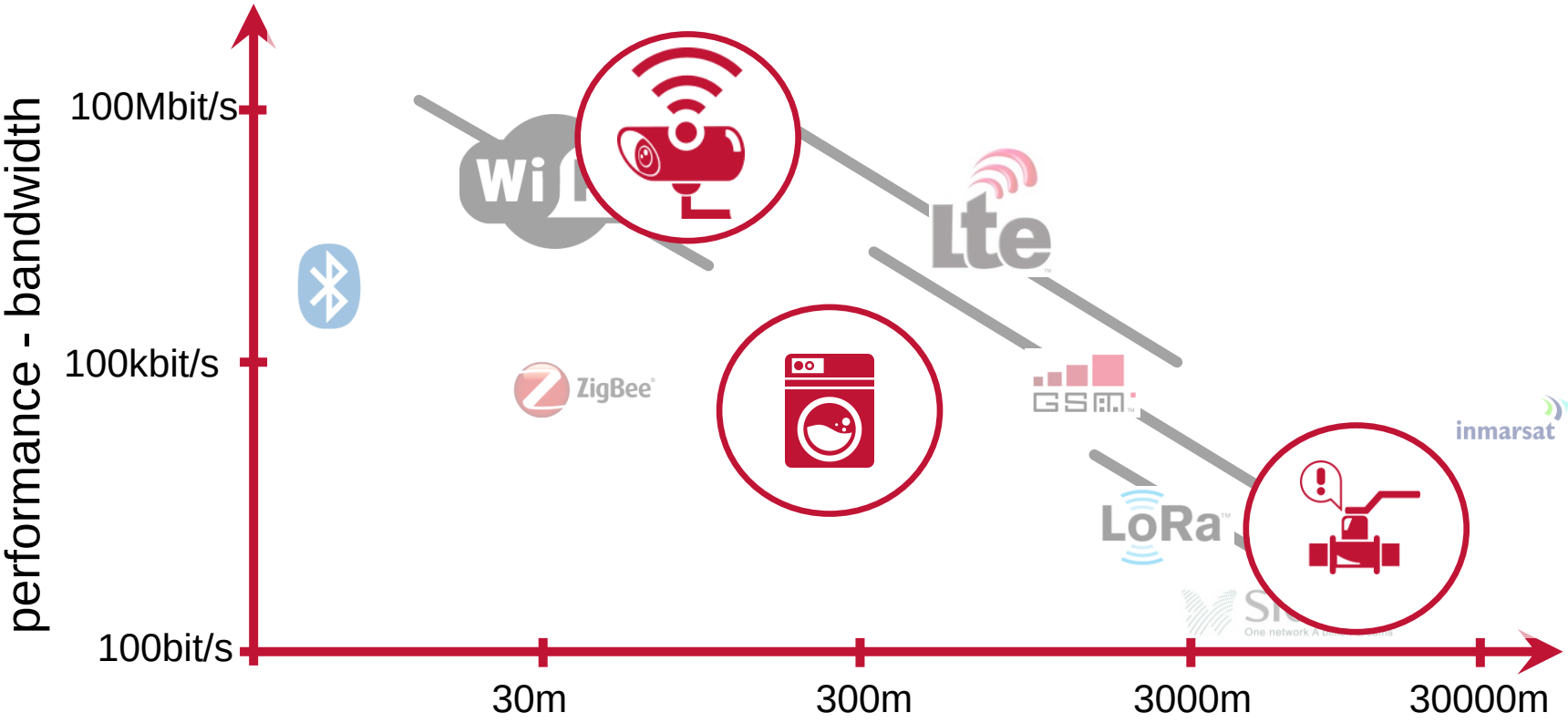
- long range and small
  - range →low frequency → large antenna

what's available?



ttp | The Technology Partnership

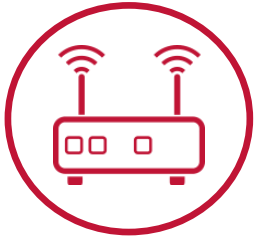
what's available?



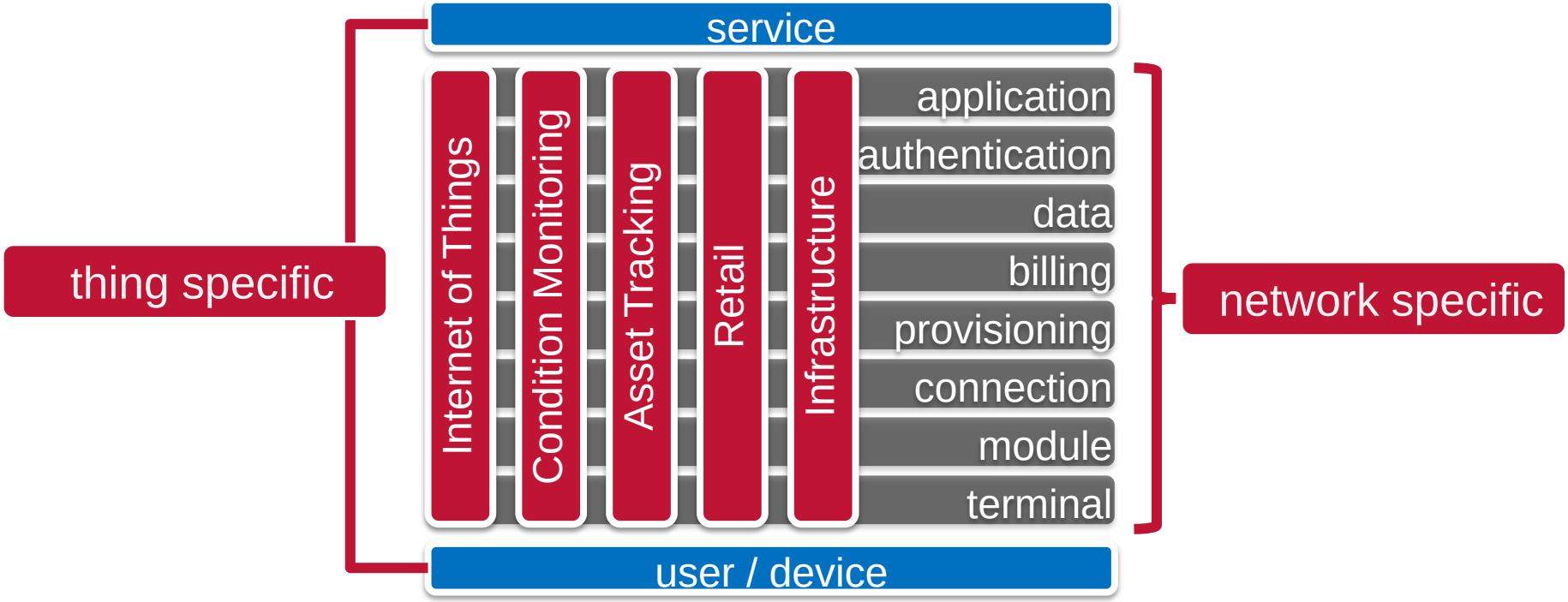
ttp | The Technology Partnership

network scale & coverage

- **where** will you need infrastructure?
  - in home, on an industrial site; for a region, a country, world wide
- **who** will provide the infrastructure?
  - the consumer, a network operator, you
- **how** many devices will you support?
  - per network, in total?
- **what**'s the platform?



what's the platform?



how secure?

- practical IoT systems do not necessarily require all possible protections in the RAN!
  - RAN attacks are limited in scale & by access
  - back-end is different
- how secure do you need to be? (what are you willing to pay for it?)
- two contrasting devices

retail label

- label cost-sensitive and battery powered
- gateways are physically secure, mains powered

- stop attackers:
  - modifying a stolen label
  - modifying transmissions - grocer fined incorrect pricing
  - decoding pricing over the air - price matching loss-making

    (but a hacker can walk into the shop…)

retail label - mitigations

- modify a stolen label
  - tamper evident design, per-node keys limit extraction and re-use
- modifying transmissions - grocer fined incorrect pricing
  - sign or encrypt network traffic, per-node keys limits damage of key loss
- decoding pricing over the air - price matching loss-making
  - encrypt network traffic

medical gateway

- some systems must protect data in the node and network
    - required by regulation for medical & financial
- some cost for hardware security is acceptable

- stop attackers:
    - reading data off a stolen device, or in transit
    - submitting fake data to network, or reading data back from network

medical gateway - mitigations

- reading data off a stolen device, or in transit
  - encrypt data at rest, in transit, (physical protection of bus?)
  - per-node keys protect the network
  - white-list or authenticate networks (don’t let the user choose)
- submitting fake data to network, reading data back from network
  - per-node keys authenticate devices
- bi-directional links allow firmware upgrade & key replacement
  - limit long-term effects of compromise

summary

- huge range of possible devices
  - with different communications and security requirements
  - some of which conflict:
    - e.g. firmware upgrade requires downlink

- RAN attacks limited in scale, but can elevate network access
  - require physical proximity (~km)

- other key questions: range, bandwidth, cost, infrastructure

for more information

ttp | The Technology Partnership

Dr Joe Milbourn
joe.milbourn@ttp.com

T +44 1763 262626 www.ttp.com