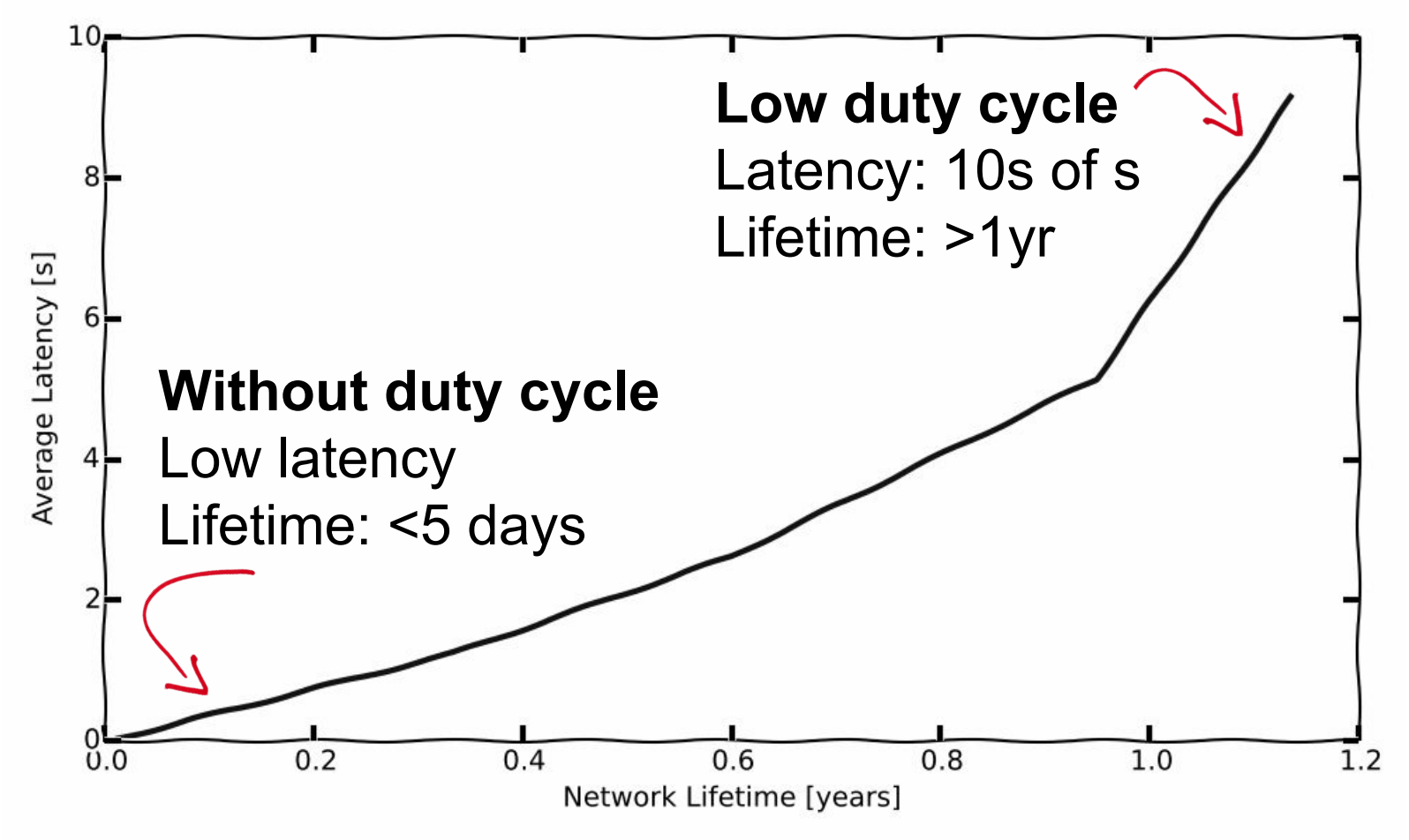
Counteracting Denial-of-Sleep Attacks in Wake-up-based Sensing Systems

Angelo T. Capossele, Valerio Cervo, Chiara Petrioli,
Dora Spenza

SAPIENZA
UNIVERSITÀ DI ROMA

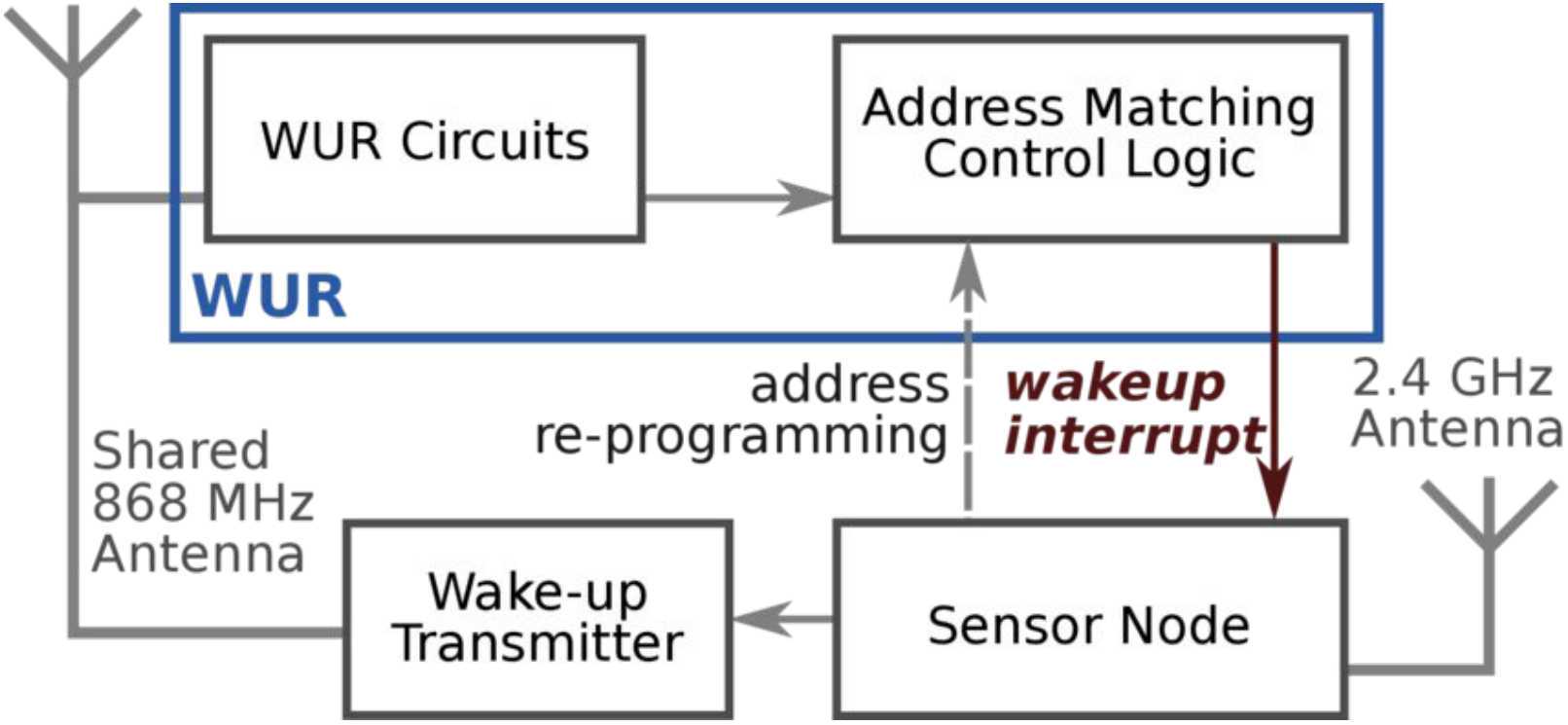
Motivation: Duty Cycling

Tradeoff between energy saving and data latency



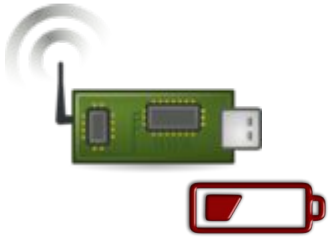
Nodes with wake-up receivers

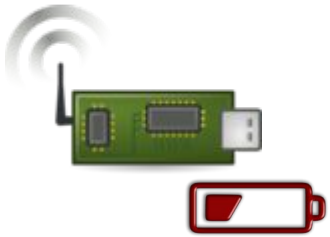
- ULP receiver continuously monitoring the channel
- Nodes sleep until communication is needed
- Selective awakenings (WUR address)

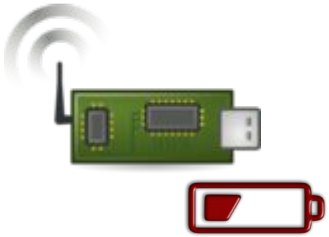


- Energy-efficient on-demand communication

The problem: Denial of Sleep attack

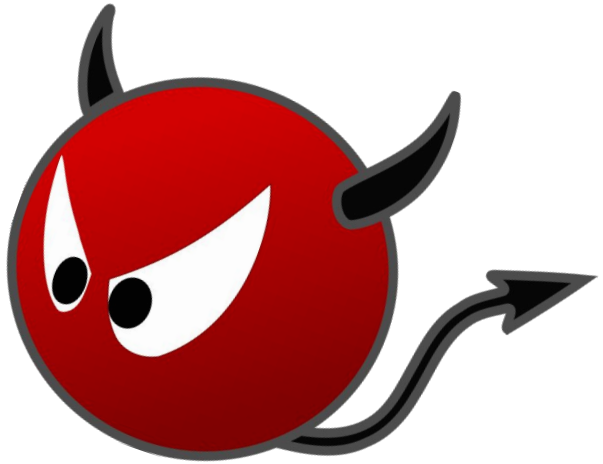






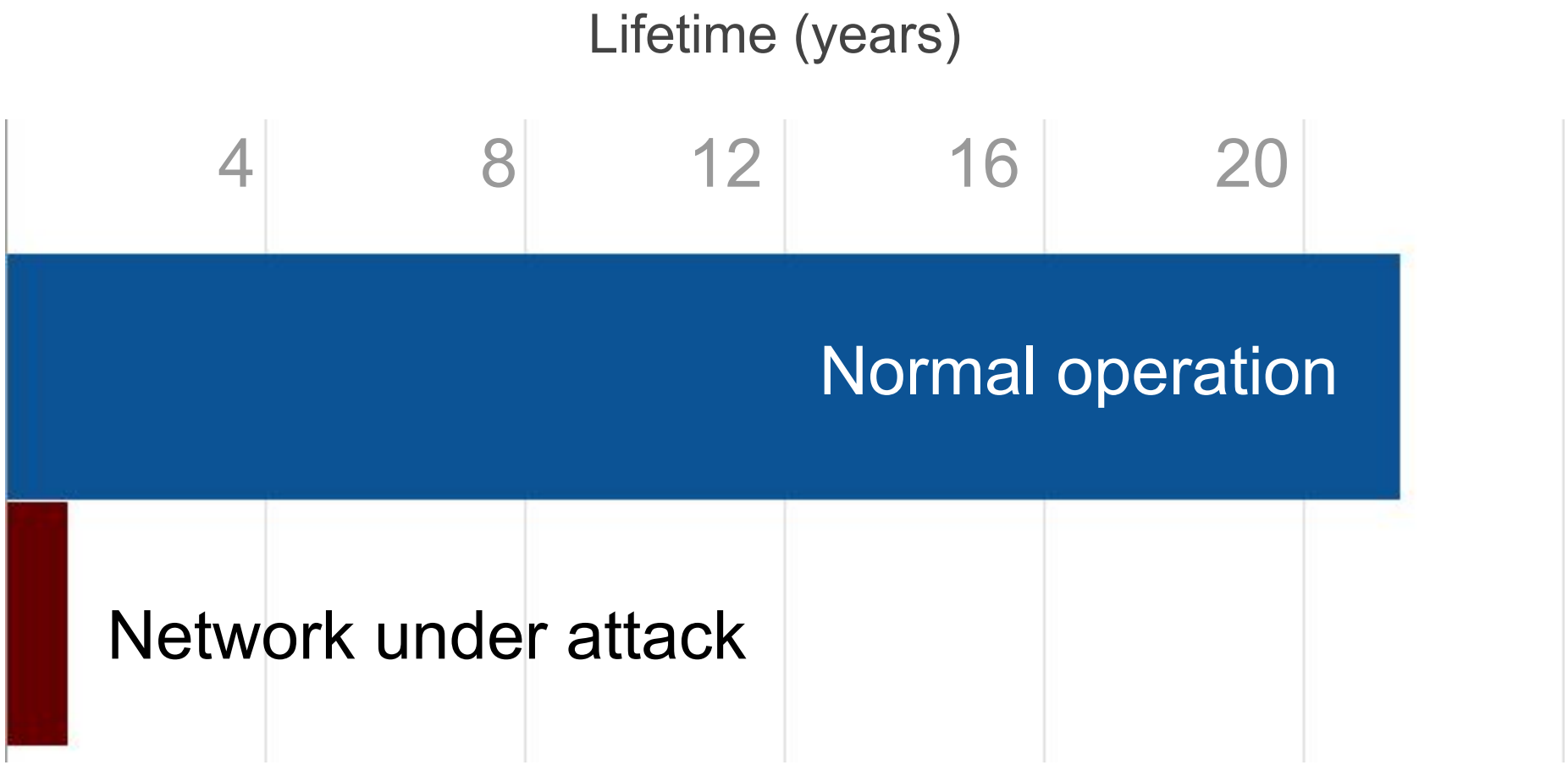
1. Bruteforce
2. Replay attack

WAKE UP!!



Effect of DoS attacks on lifetime

Single attacker: replay attack every 10s



Our solution: AntiDoS

Secure wake ups only from authorized nodes

Prevent replay attack

WUR addresses updated in a pseudo-random fashion after every use

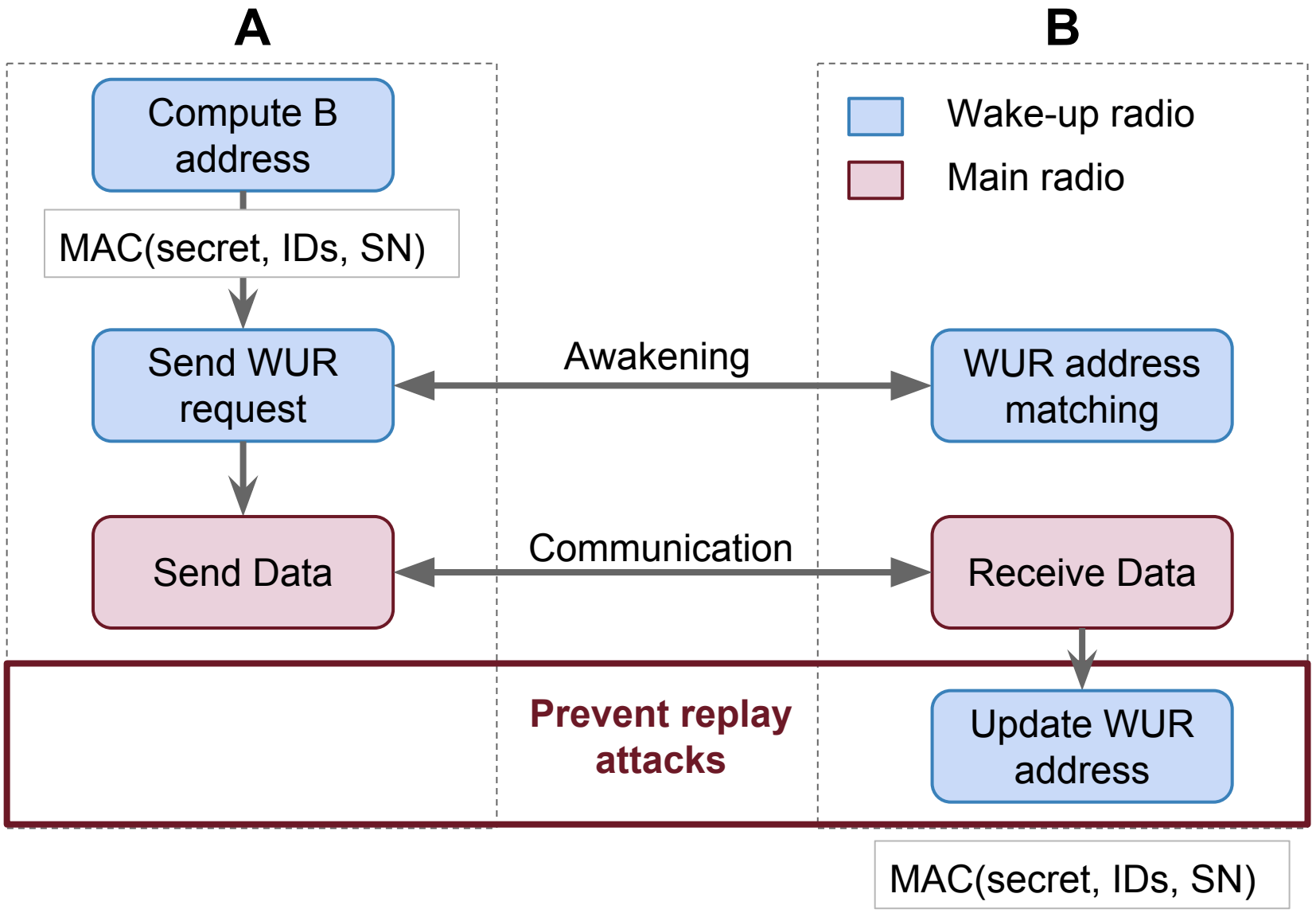
MAC(common secret key, ...)

Bootstrap phase

Key Management Protocol

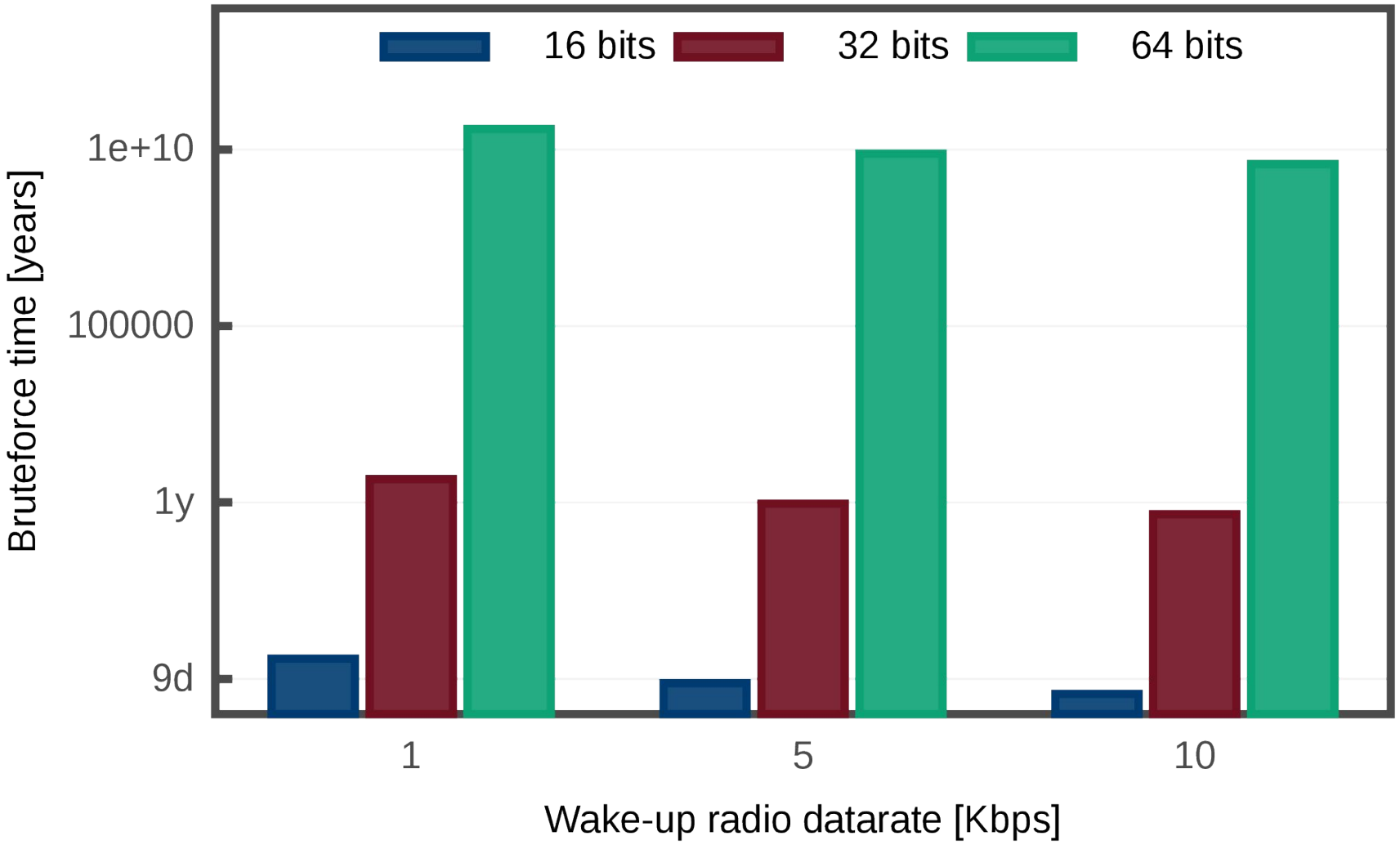
- Lightweight
- Mutual authentication

AntiDoS protocol (unicast)



Bruteforce

Attacker must use datarate of the WUR

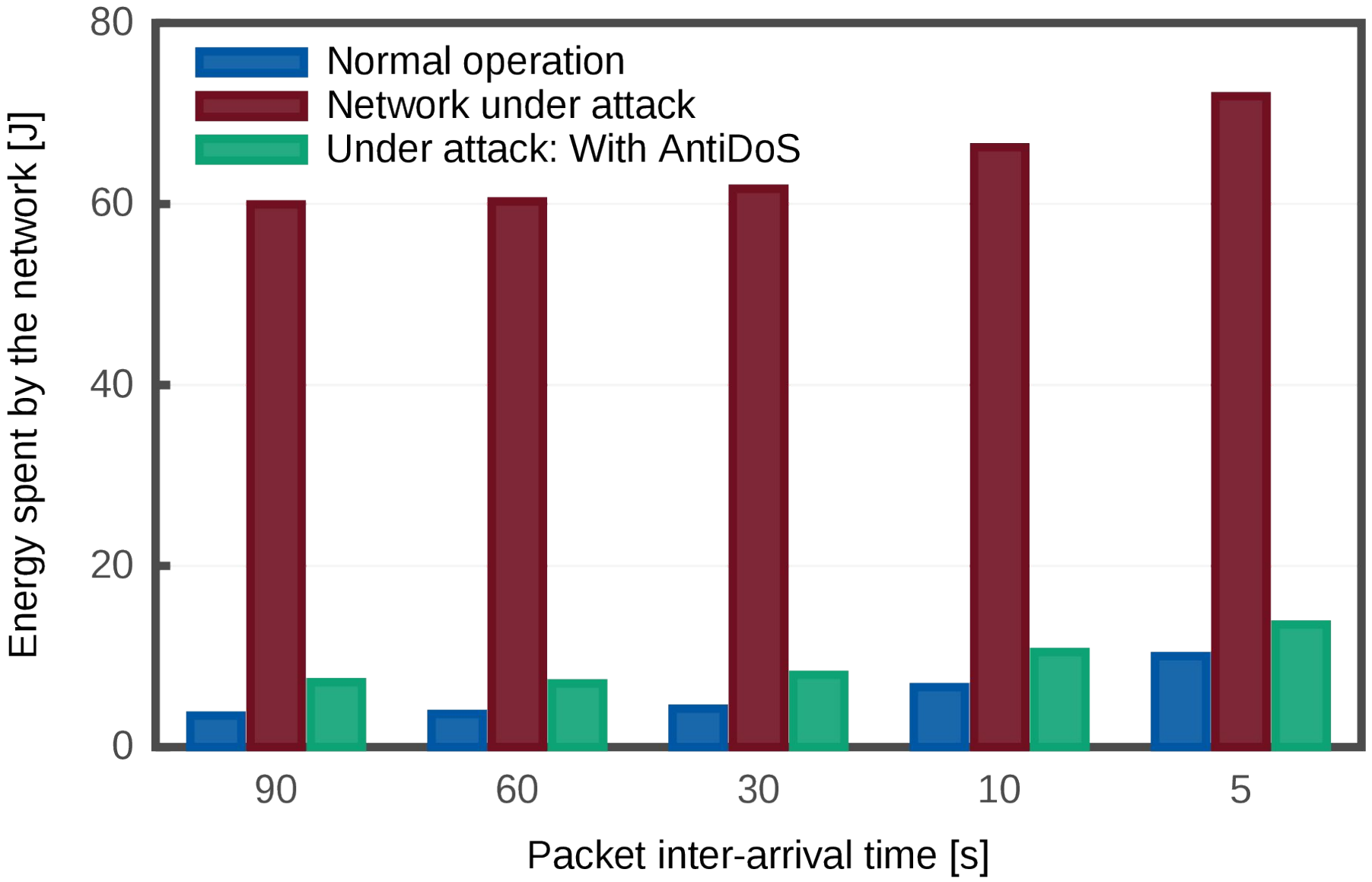


Simulation setup

- Simulation framework: GreenCastalia
- WUR model: actual prototype, experimental data

- Monitoring application, converge casting (CTP)
- Single attacker randomly placed in the field
- Overhear legitimate WUR addresses
- Re-broadcast them every 10s to prevent nodes from sleeping

Simulations results: Energy



Experimental validation

- MagoNode++
  - WUR
  - Energy harvesting

- TinyOS implementation

Energy consumption of AntiDos operations

- Scalar addition/multiplication 14 uJ
- SHA-160 0.04 mJ
- HMAC 0.28 mJ

...

Conclusion

Denial of Sleep attacks are a significant threat for WUR-based sensing systems

AntiDos

- Secure wake ups (authorized nodes)
- “Disposable” WUR addresses thwarts replay attacks

Thank you!