Group Communication Security for Low-Power and Lossy Networks

draft-keoh-dice-multicast-security-08

draft-kumar-dice-groupcomm-security-00

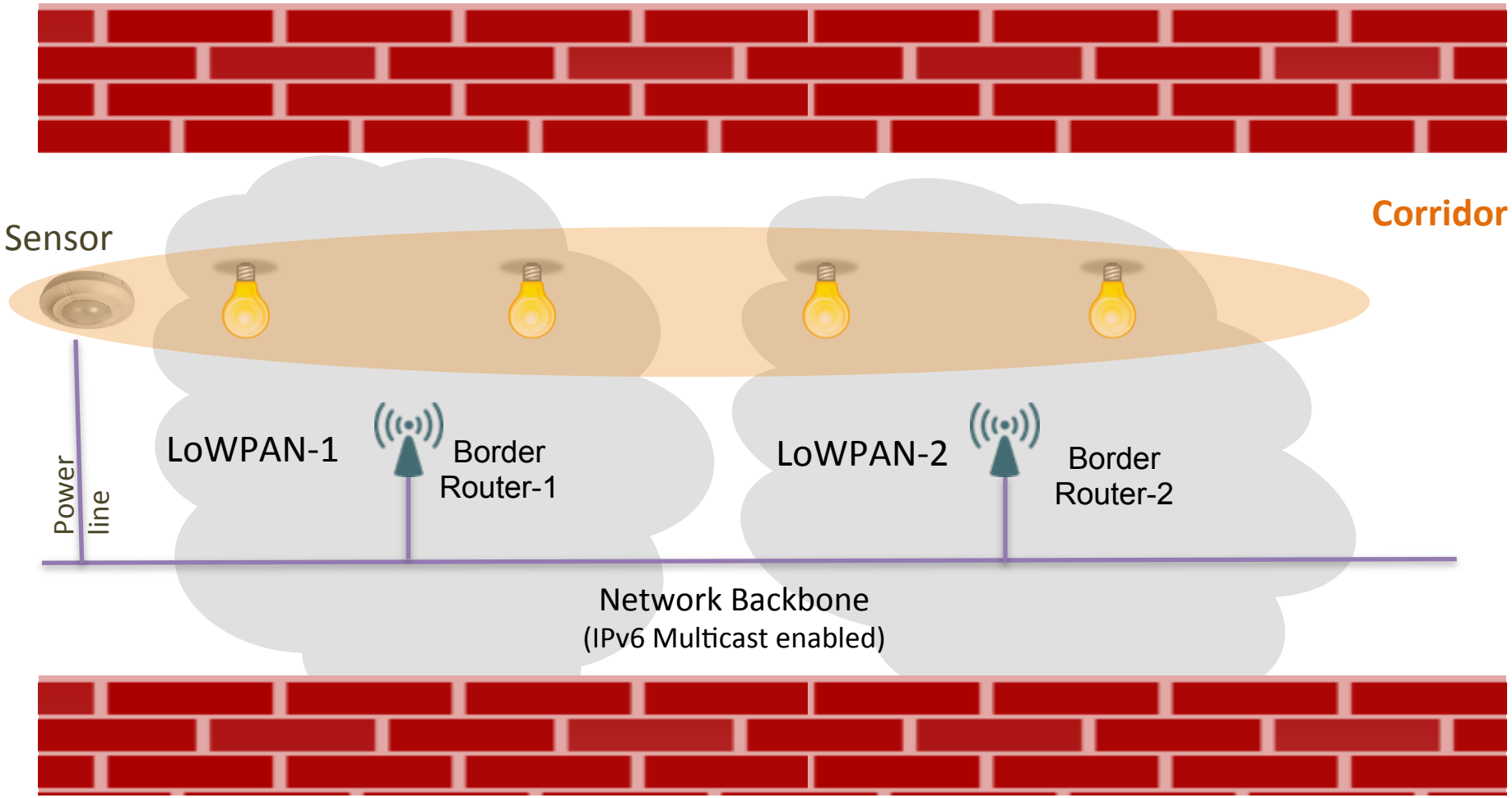
Sandeep S. Kumar

IETF90 July 22, 2014, London

Email: sandeep.kumar AT philips.com

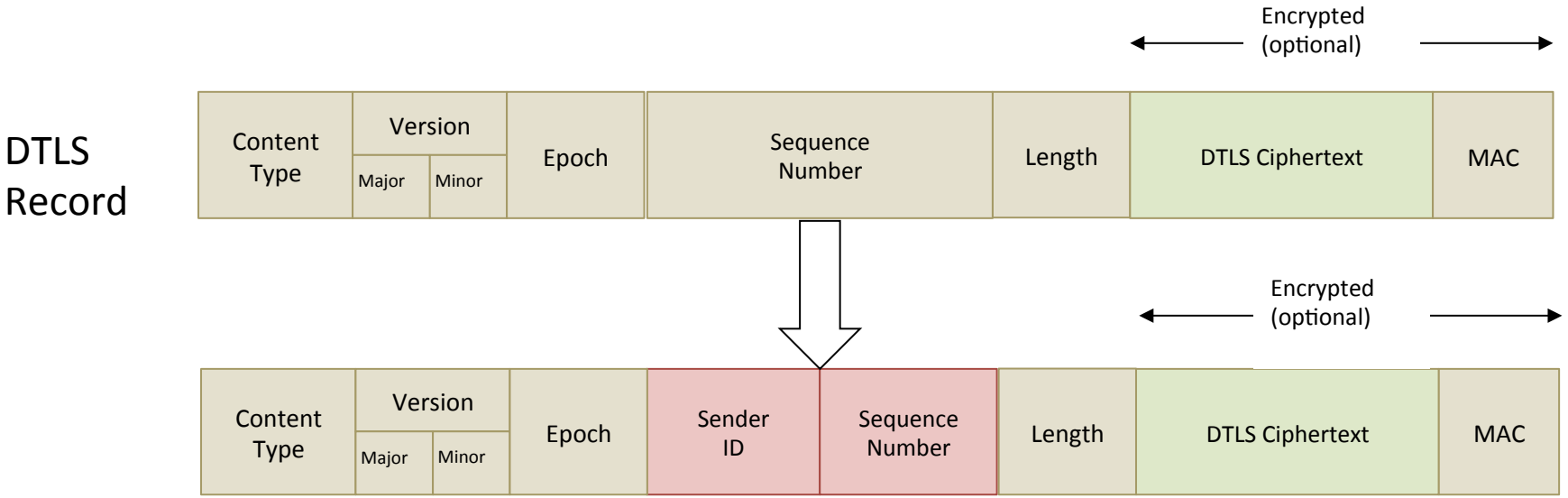
Group Communication Use Case

Lighting control in Office Building



Symmetric key based (recap)

Use DTLS record layer to also protect CoAP group communication messages (in addition to CoAP unicast)



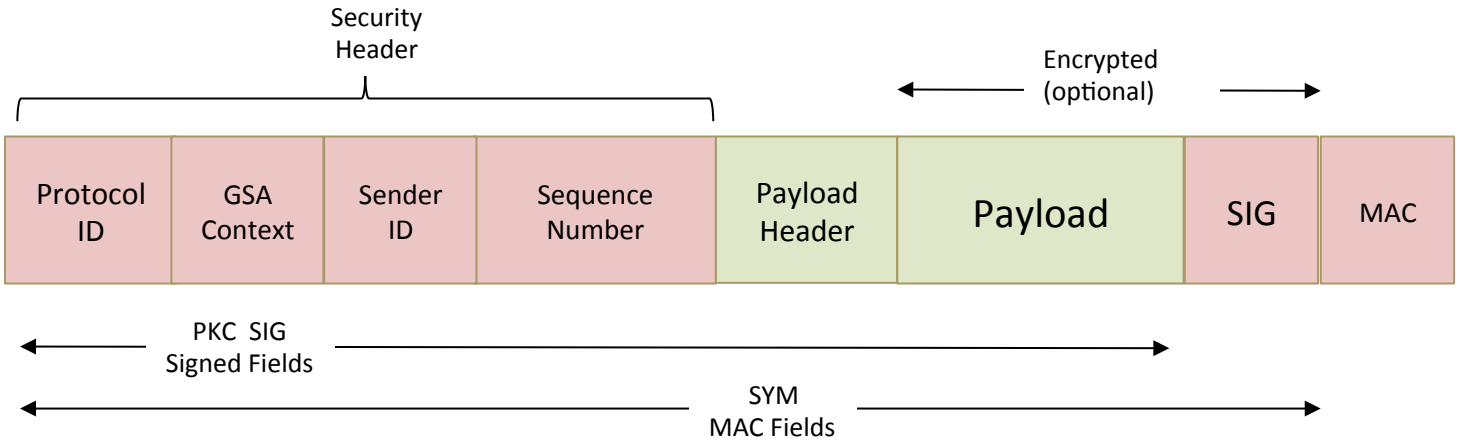
Symmetric key based (updates)

- Explicitly limit the group size < 100 nodes
- Constrained the draft scope to lighting only
- Identify how to cope with responses (if any)
  - Follow CoAP RFC recommendations based on matching Token values
- Handling in the presence of a (forward) proxy

Public key based solution

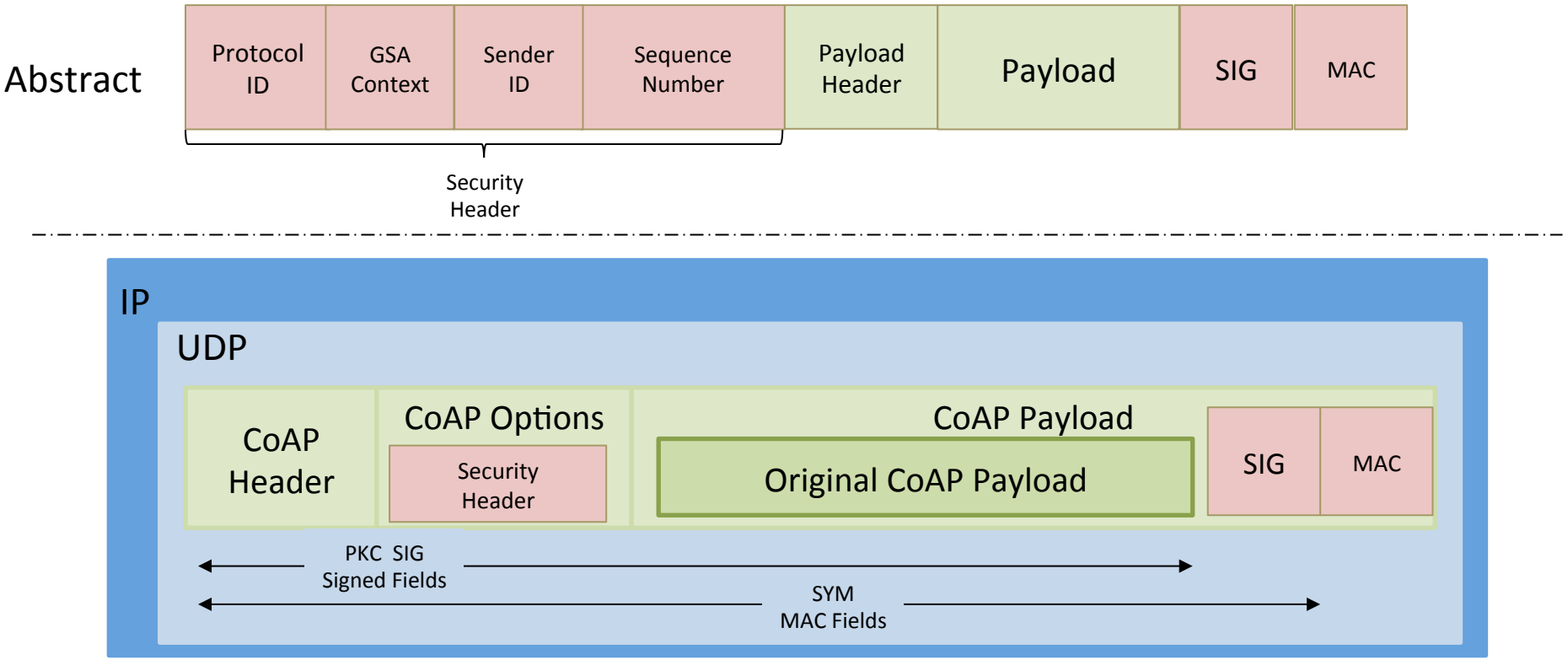
Abstract depiction of what is needed

- SIG – signature based on public key crypto
- MAC – message authentication code based on symmetric group key

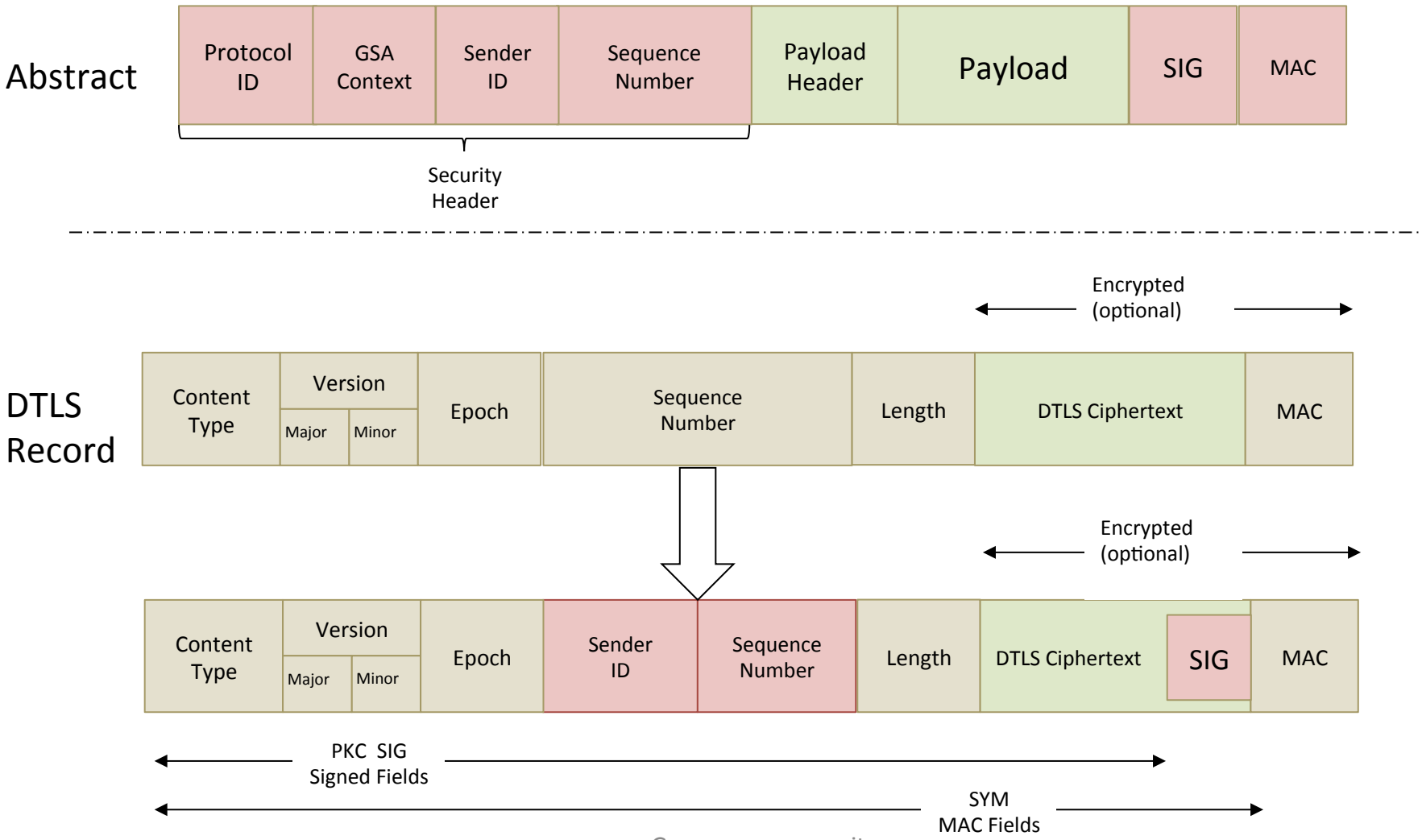


Solution specific to CoAP

Protect CoAP headers
Use CoAP Options to indicate group security



Optionally in DTLS layer



Public key option

- Per message
  - Signature size? (use smaller key strengths)
  - Computation
    - Latency? (precomputation?)
    - Power? (DoS for battery operated devices)
    - Code-size/memory?

Public key options

- Group security inside CoAP
  - CoAP layer changes?
- In the DTLS layer
  - Transparent to CoAP
  - Applicable to possibly other application messages