DTLS-based Multicast Security for Low-Power and Lossy Networks (LLNs)

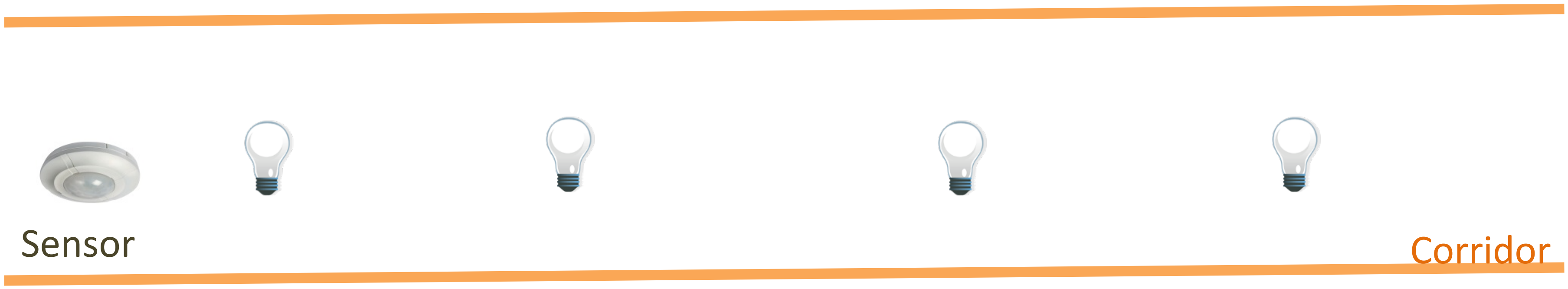
draft-keoh-dice-multicast-security

Sandeep S. Kumar, *Sye Loong Keoh, Oscar Garcia-Morchon,*
Esko Dijk, Akbar Rahman

IETF89 March 3, 2014, London
Email: sandeep.kumar AT philips.com

Group Communication Use Case

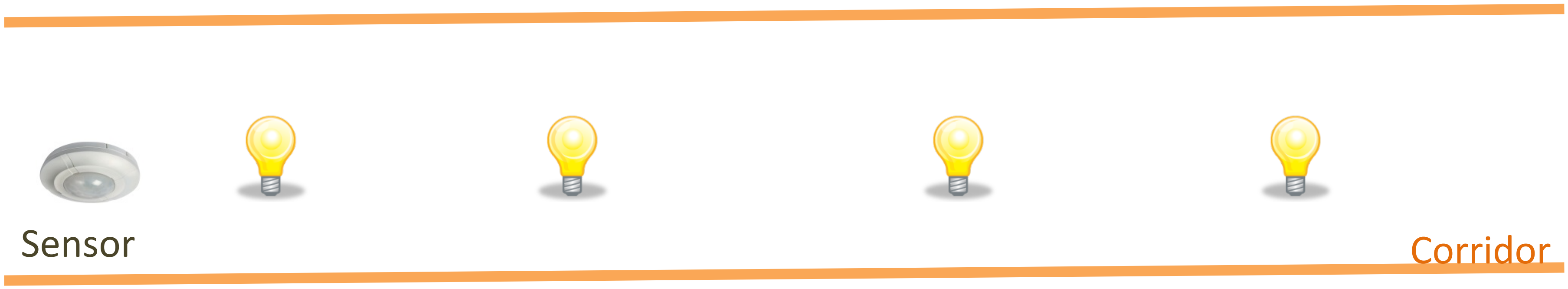
Lighting control



Group Communication Use Case

Lighting control

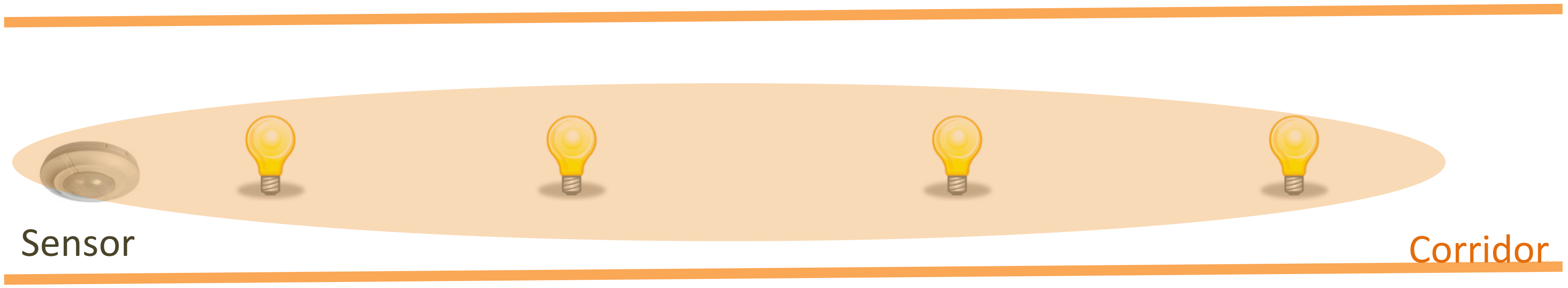
- Visually synchronous change



Group Communication Use Case

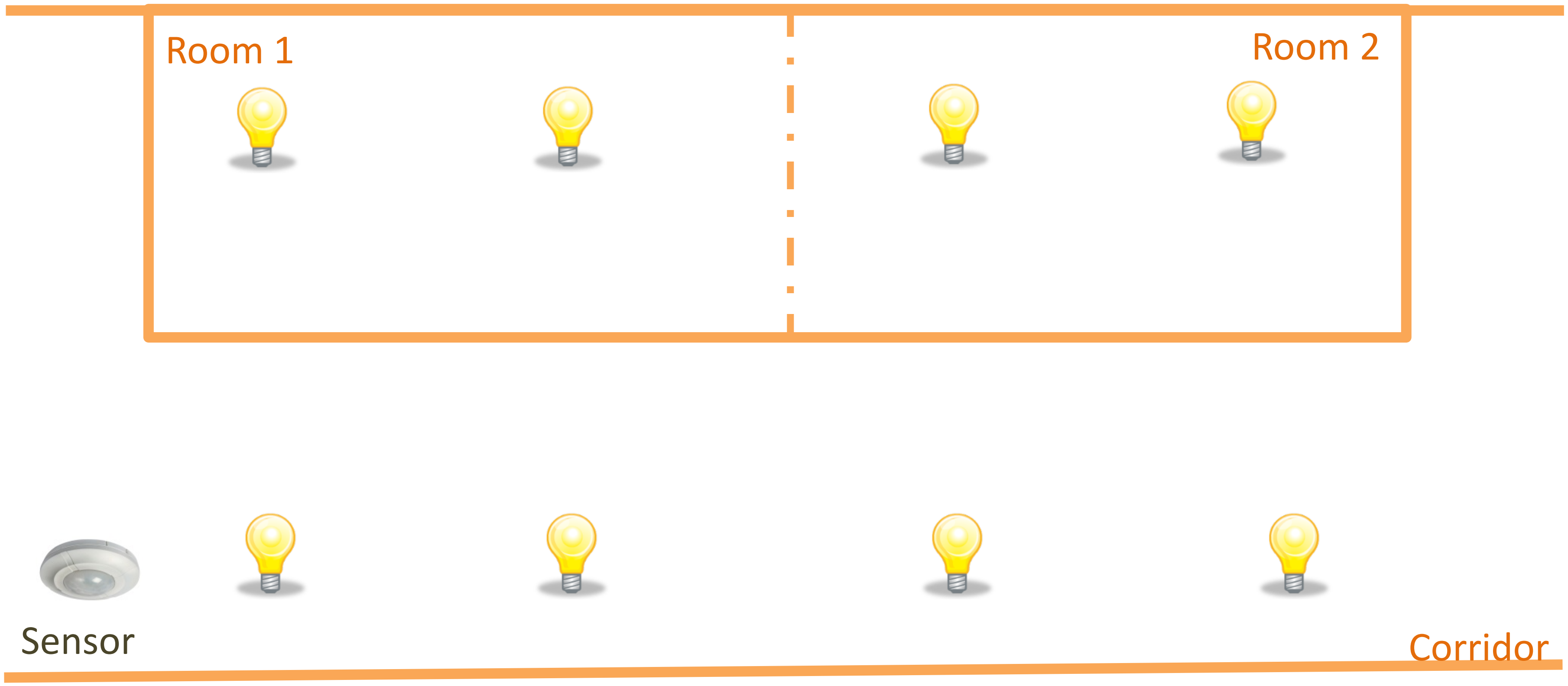
Lighting control

- Visually synchronous change
- Multicast groups -> CoAP group communication



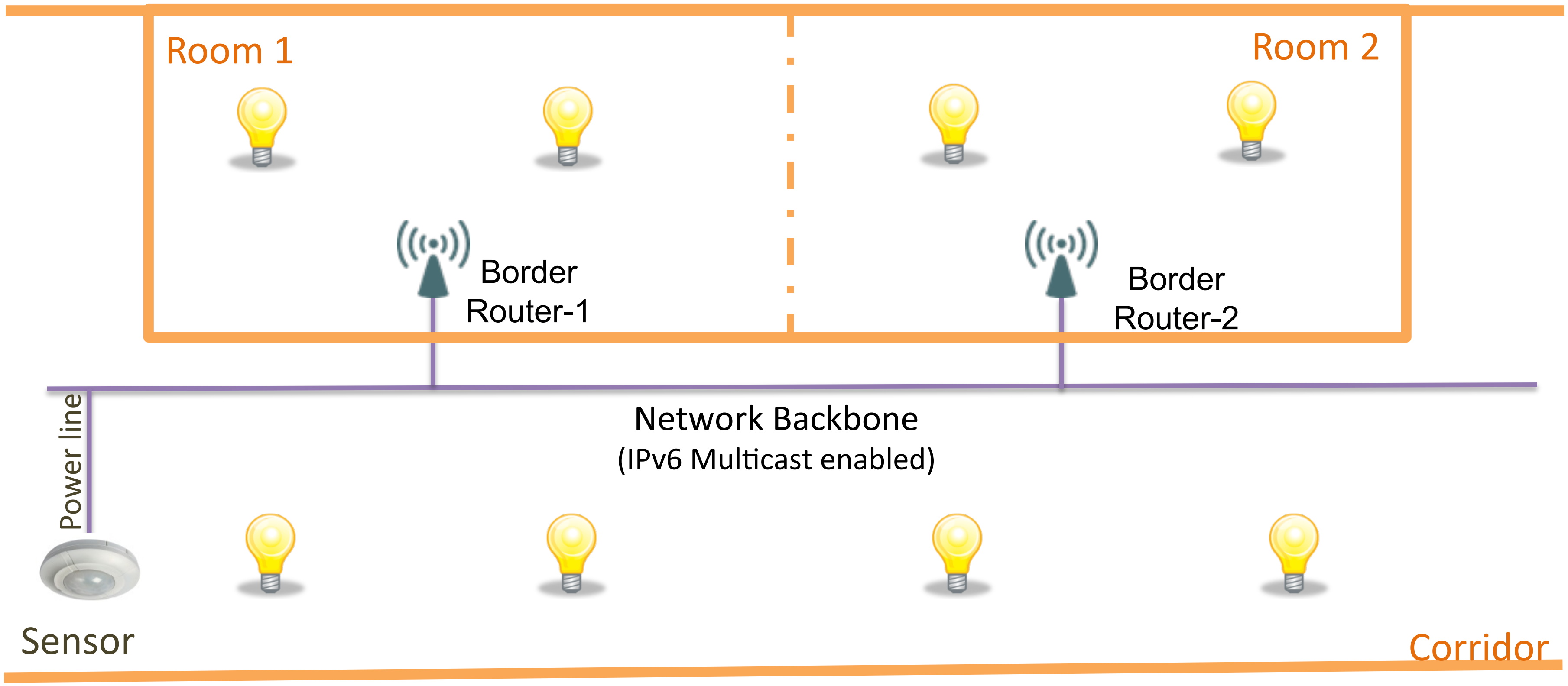
Group Communication Use Case

Lighting control in Office Building



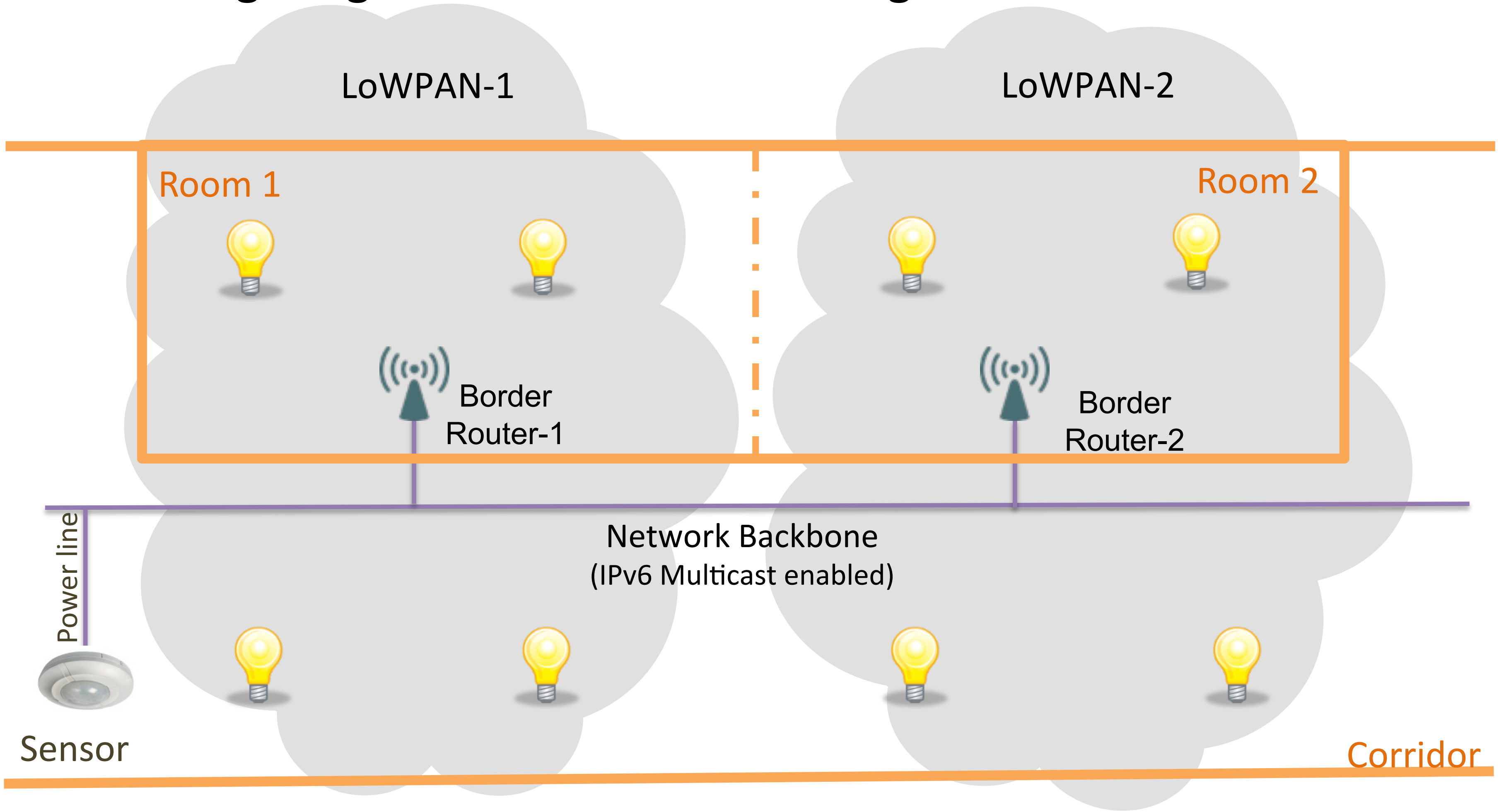
Group Communication Use Case

Lighting control in Office Building



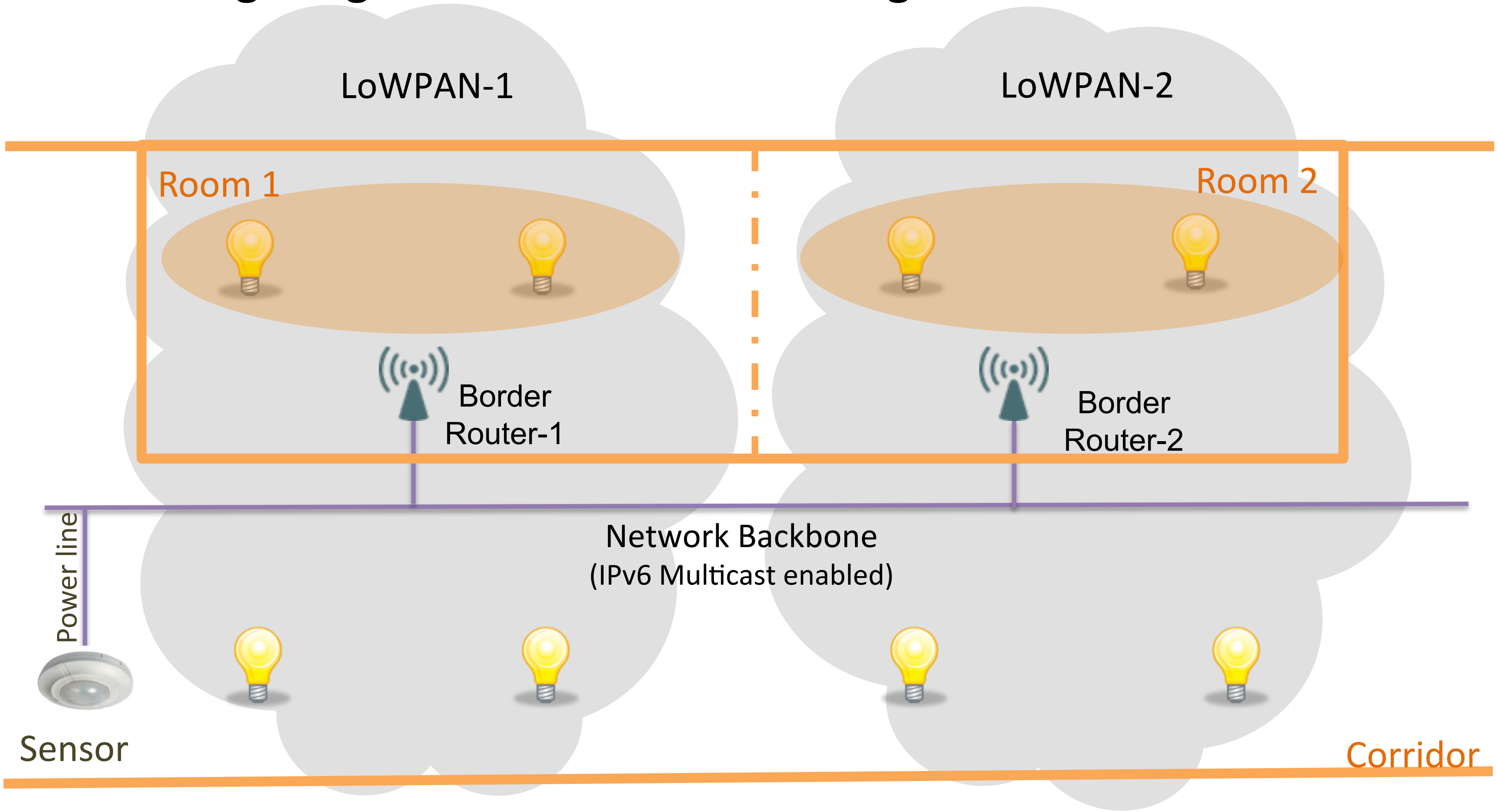
Group Communication Use Case

Lighting control in Office Building



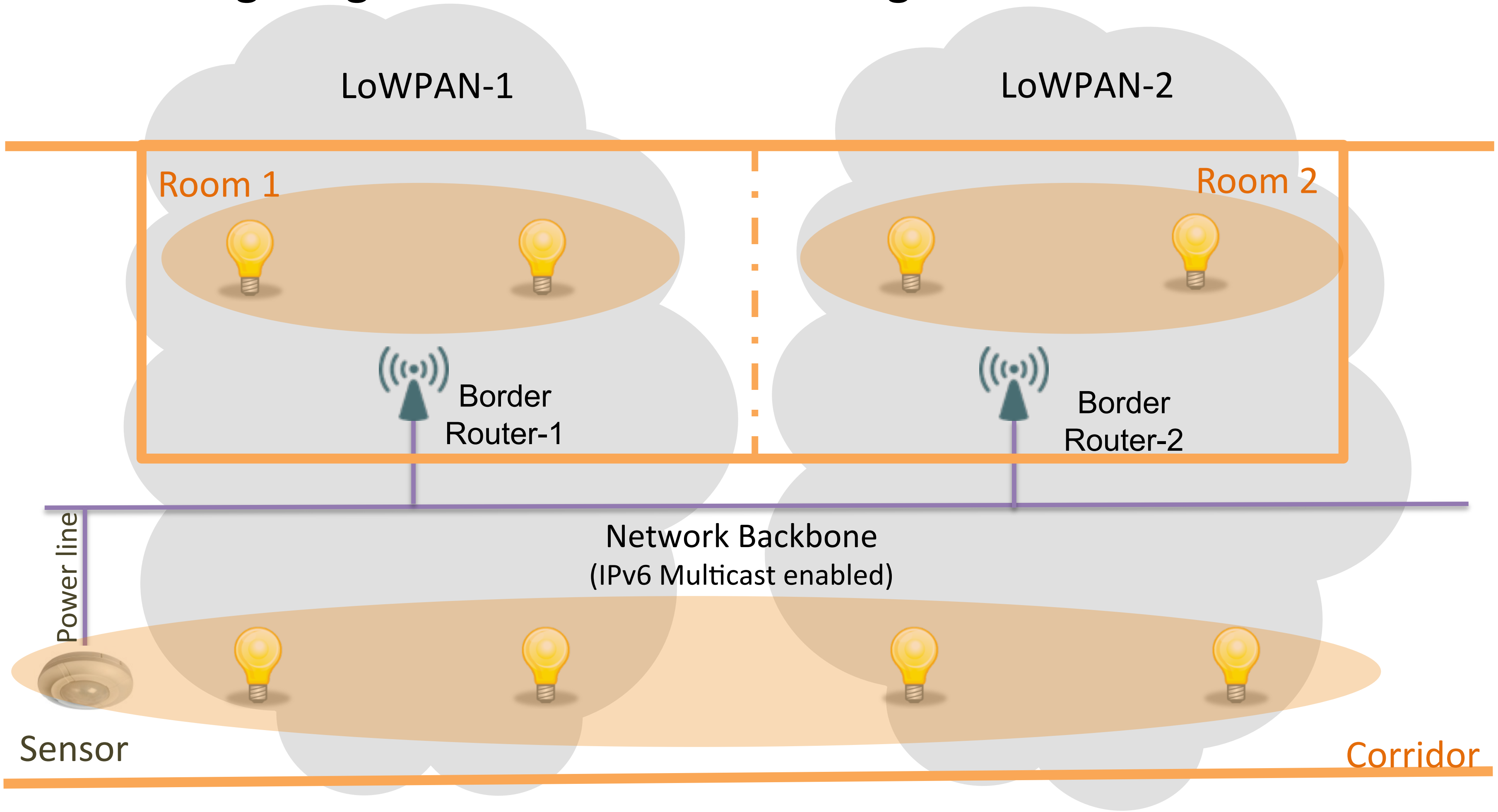
Group Communication Use Case

Lighting control in Office Building



Group Communication Use Case

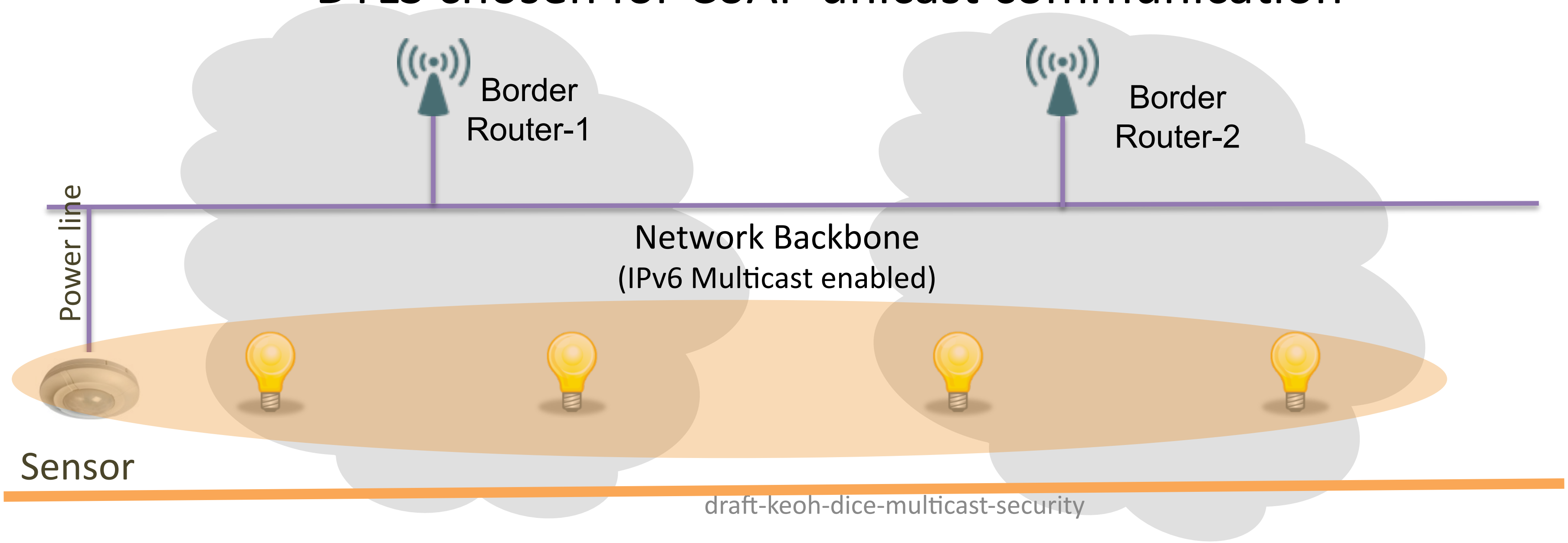
Lighting control in Office Building



Requirement

Security for CoAP group communication messages across multiple LowPANs/PHY-networks

- Same security level as within a single LowPAN
- Groups of <100 nodes
- Group level Confidentiality, Integrity, Replay protection
- Reuse existing protocols on constrained devices
  - DTLS chosen for CoAP unicast communication

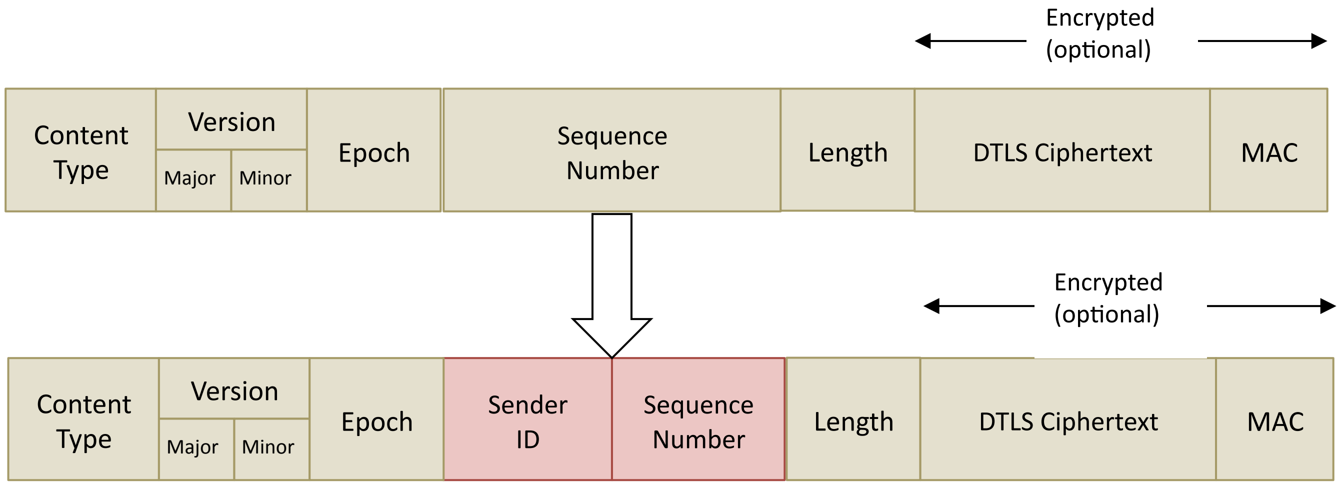


Proposed solution

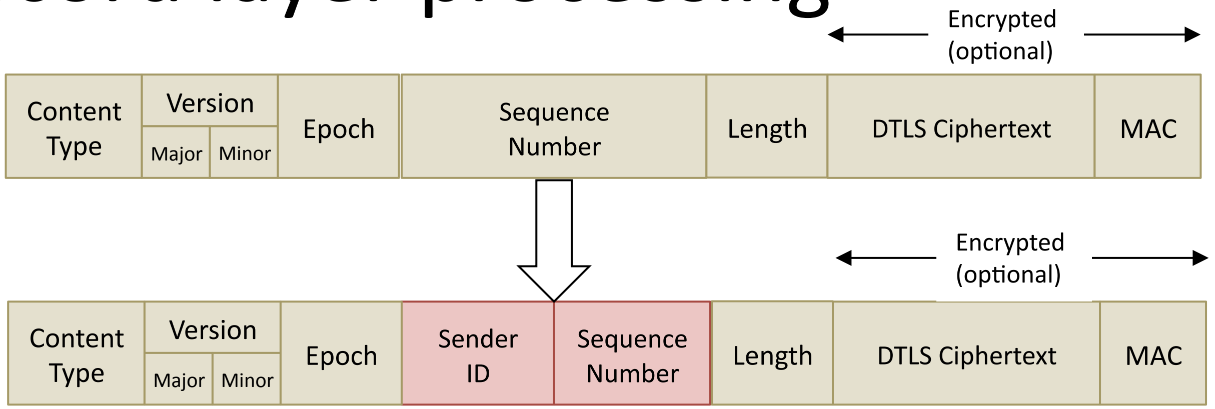
- Use DTLS record layer to also protect CoAP group communication messages (in addition to CoAP unicast)
- Out-of-band setup of Groups Security Association (GSA) for group members
- Support multiple senders in the group
  - Adapt DTLS record layer to avoid reuse of nonce for AEAD cipher suites

DTLS record layer adaptation

- Each sender gets a *unique* ***SenderID (1-byte)*** from the group controller
- In the DTLS Record Layer, split the ***6-byte*** *sequence number* field into:
  - ***1 byte*** *Sender ID* and ***5 bytes*** *"truncated" sequence number*.



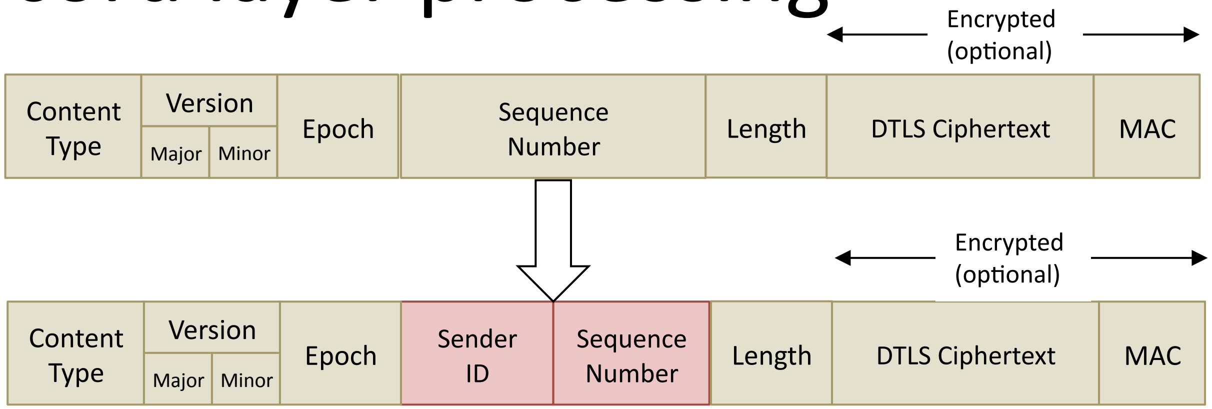
DTLS record layer processing



Senders

- "write state" is instantiated with "server write" parameters.
- Each sender manages its own *epoch* and "truncated" *sequence number*
  - no synchronization is needed with other senders in the group. Initialized to 0.
- The sender include its *Sender ID* in the DTLS Record Layer header and increments the "truncated" sequence number when sending a group message.
- The *epoch* will be increased, and the "trunc." *sequence number* will be reset once the group session key is renewed or updated (*out-of-scope: to be defined as part of key management*)

DTLS record layer processing



Listeners (Receivers)

•Multiple “read states” are instantiated with “server write” parameters for each sender linked by *SenderID*

- Keying material same but the epoch and the "truncated" sequence number of the last received packets needs to be kept different for different senders.

•Listeners use the *multicast destination IP and port address* of the packet to lookup the “server write” key.

•Message is decrypted and the MAC of the message is checked

•Using the *Sender ID* field, receivers retrieve the last used *epoch* and *sequence number* to detect replayed messages.

- If success: last seen seq number from the SenderID in the “read state” is updated

Changes since IETF 88

- More discussion on the group level security
  - Security considerations provide additional guidance on the risks of single group key
- Limit number of group members < 100
  - SenderID field reduced from 2-bytes to 1-byte
- Ensure the solution is crypto-agile
  - Not limited to any particular cryptosuite like AERO
  - Supports DTLS cryptosuites used at record layer
- Other comments
  - Use port address for binding

Summary

- Group communication requires application security in many scenarios

- Preferably re-use existing security protocols on constrained devices in LLNs.

- Proposal to reuse DTLS Record layer to support secure group communication.