Multicast Security for the Lighting Domain

somaraju-ace-multicast

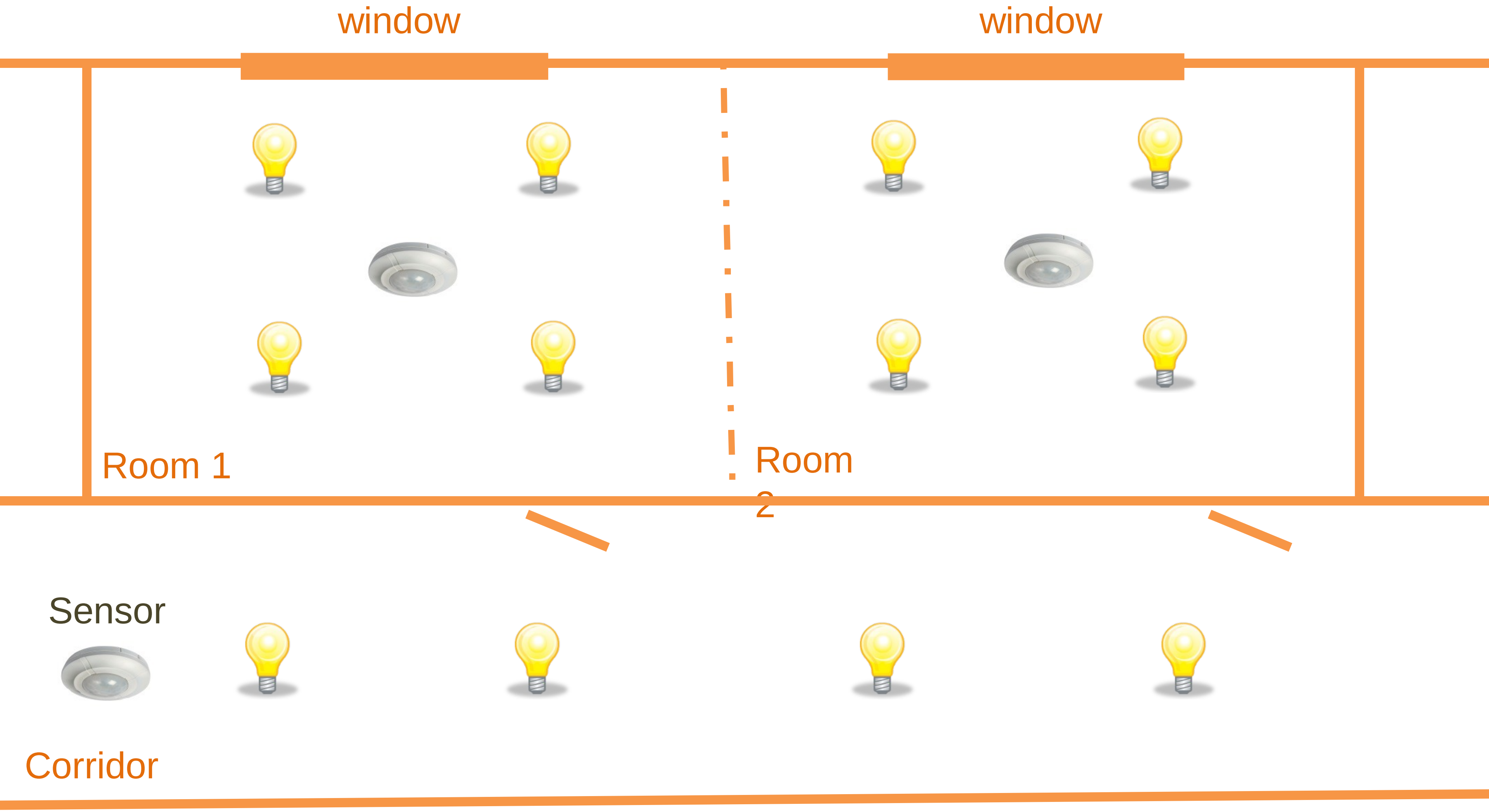
Abhinav Somaraju

Sandeep S. Kumar

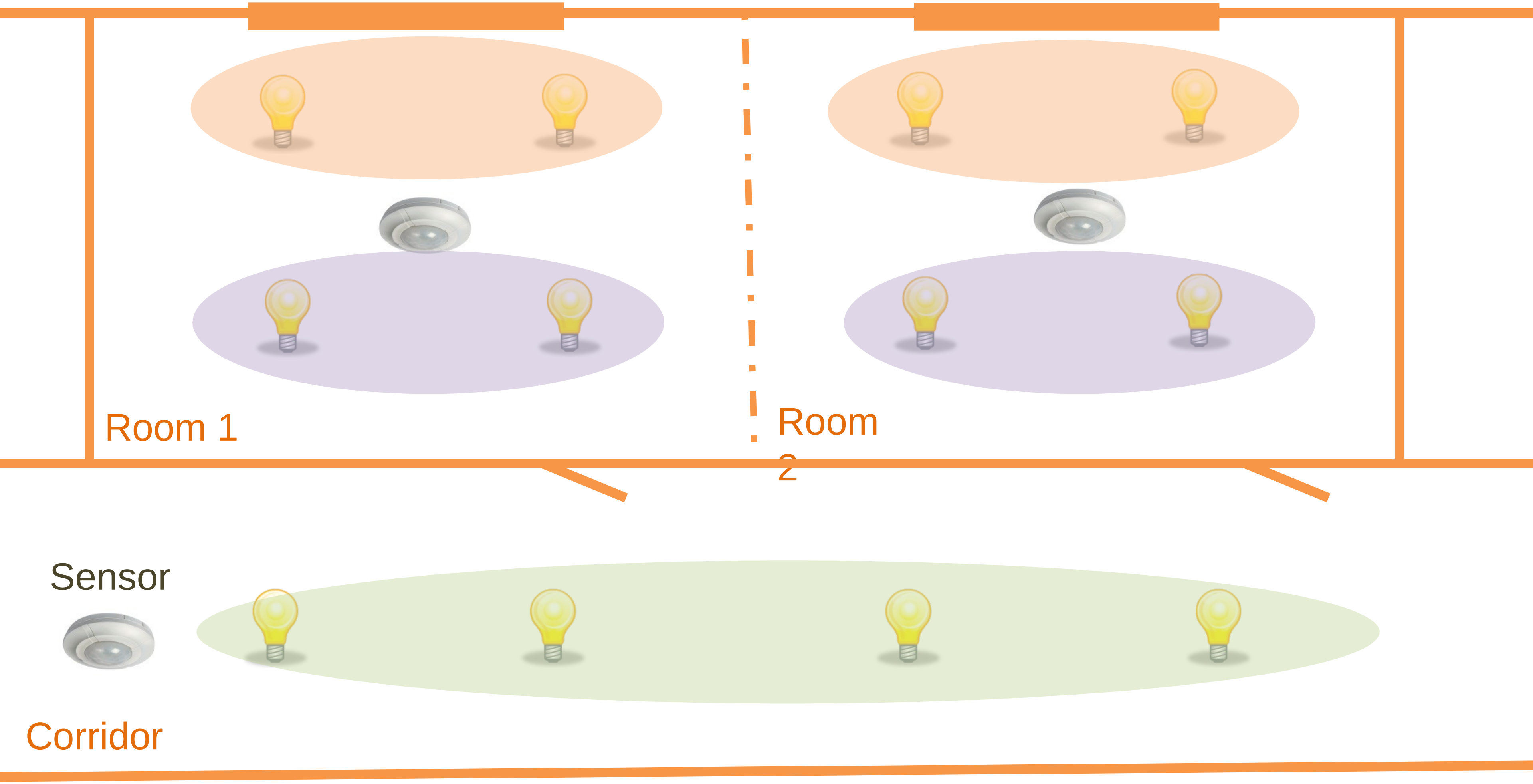
Hannes Tschofenig

OpenAIS /Open Architectures for Intelligent Solid State Lighting Systems

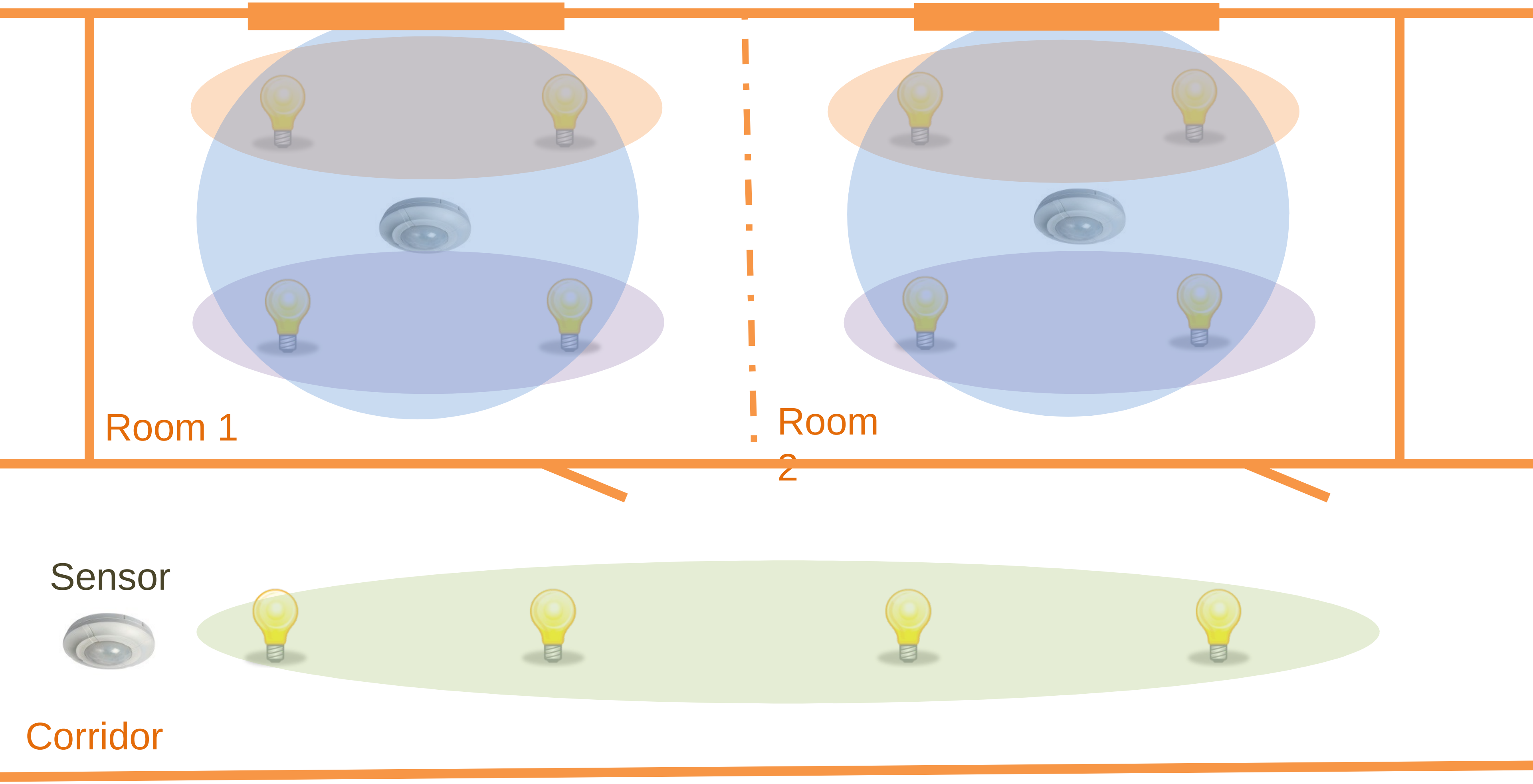
A typical professional lighting system



A typical professional lighting system



A typical professional lighting system



System level requirements

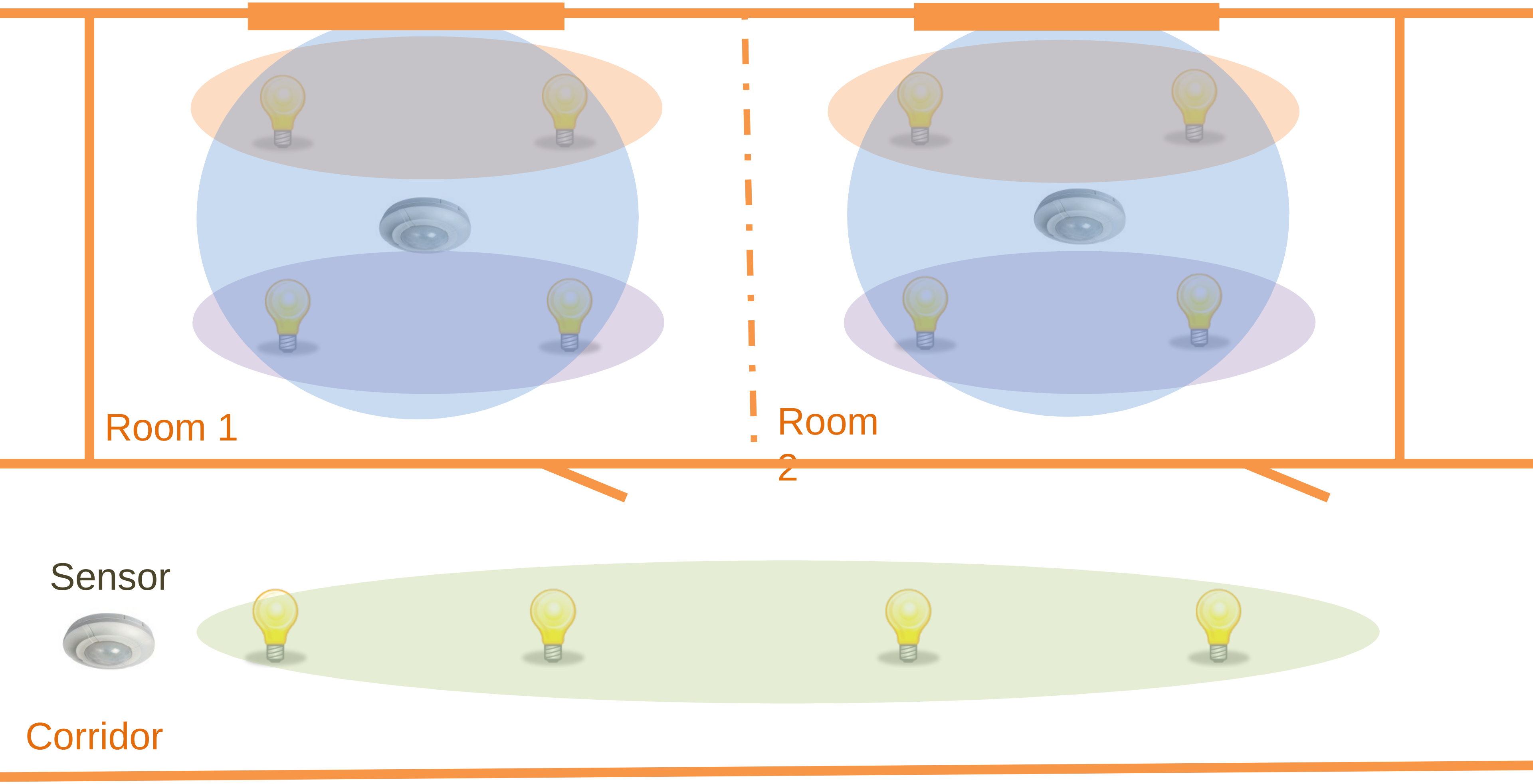
Three requirements (relevant to security) need to be addressed for group communication:

1. Only authorized members of the application group must be able read and process messages.
2. Receivers of group messages must be able to verify the integrity of received messages as being generated within the group.
3. Usually, message transfer and processing must happen with low latency and in synchronous manner (typically latency less than 200 ms and jitter less than 50 ms).

Group concept

- **Application group**
  - A lighting application group that consists of the set of all lighting devices that have been configured by a commissioner to respond to events in a consistent manner.
- **Multicast group**
  - A multicast group consists of the set of all nodes that subscribe to the same multicast IP address.
- **Security group**
  - A security group consists of a set of sending and receiving nodes such that any sending node is able to securely send a message to all the receiving nodes.

Multicast vs Application vs Security Groups



Typical lighting systems workflow

- **Installation**: Fix devices, electrically connect, install network wires (if wired)
- **Commissioning**: Assign logical address, configure groups and behavior
  - Often the backend infrastructure may yet need to be installed and connected
- **Operational**: Choose preassigned behavior
  - Commissioning Tool is no more available

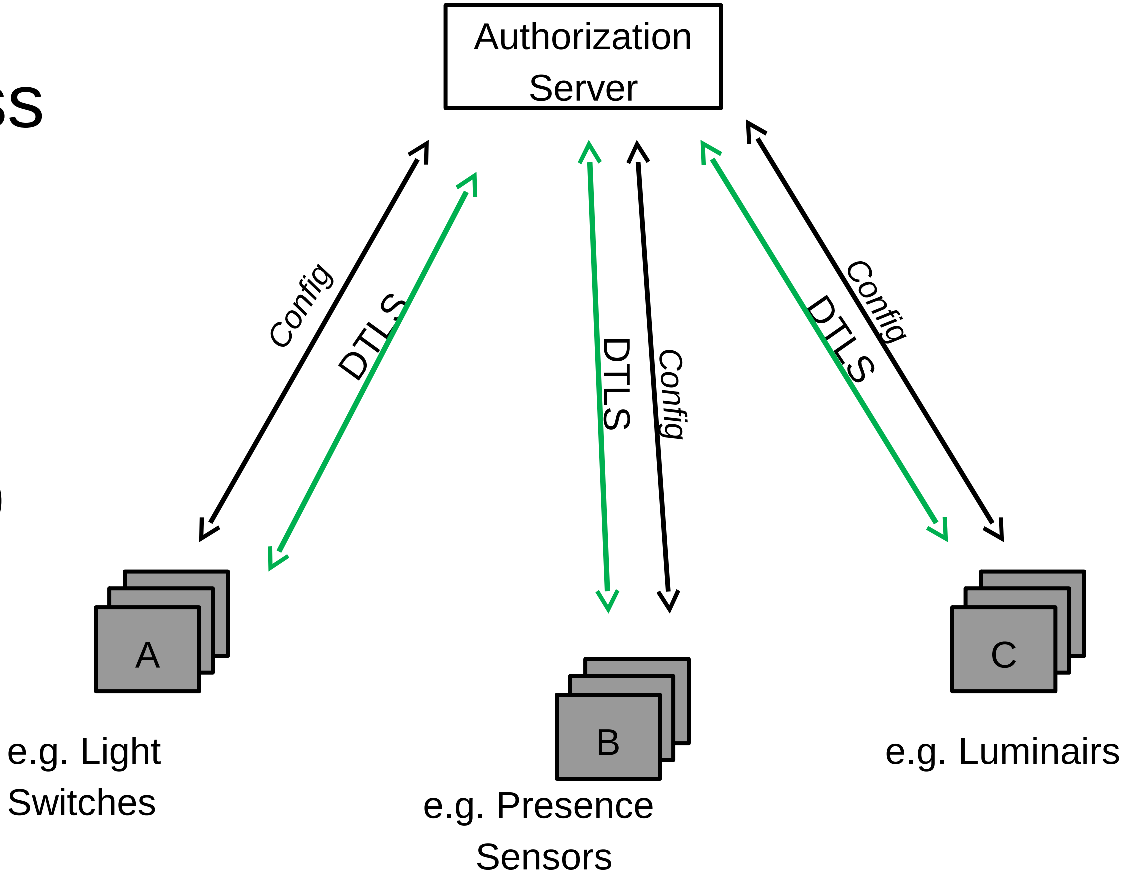
Security design

- Two step process

<u>1st step</u>

Commissioning

  - Access Tokens for KDC (AT-KDC)



***Config** (Configuration Data): Includes configuration parameters, authorization information encapsulated inside the access token (AT-KDC) and other meta-data*

Security Design

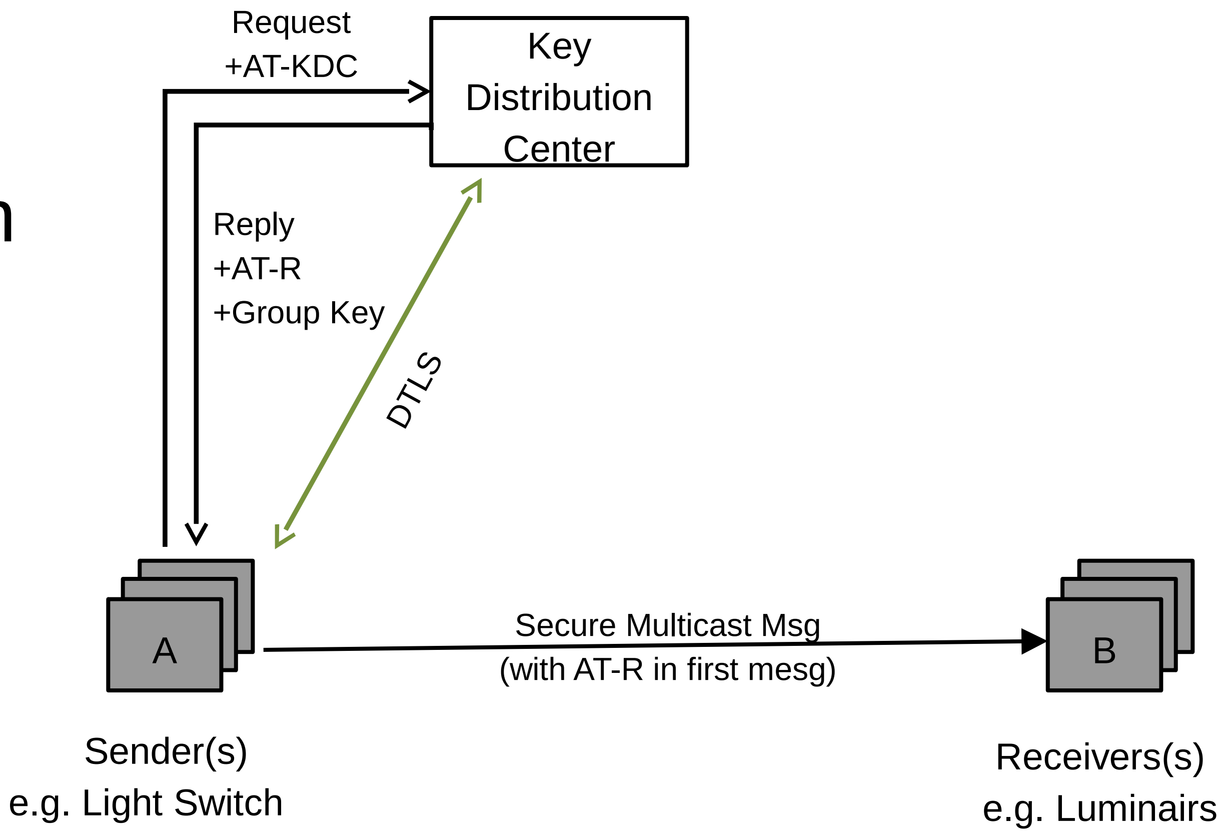
<u>2nd step</u>

Operational

Access Token

for Resource

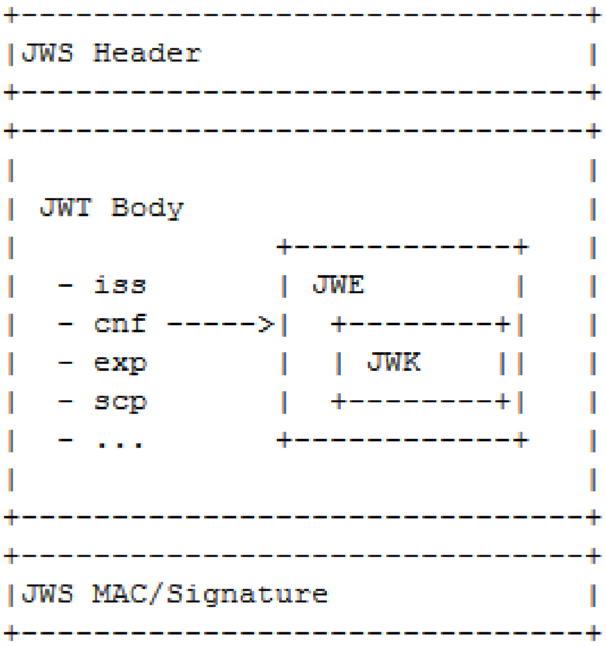
(AT-R)



Secure Multicast messaging either using
transport security or using object security

Access tokens

- AT-KDC: Bearer token
- AT-R: Proof-of-Possession (PoP) token



```
+-------------------------------+
|JWS Header                     |
+-------------------------------+
+-------------------------------+
|                               |
|  JWT Body                     |
|              +------------+   |
|  - iss       | JWE        |   |
|  - cnf ----->|  +--------+|   |
|  - exp       |  | JWK    ||   |
|  - scp       |  +--------+|   |
|  - ...       +------------+   |
|                               |
+-------------------------------+
+-------------------------------+
|JWS MAC/Signature              |
+-------------------------------+
```

Still need to work out details of the token, like scope etc.

Open issues- work in progress

- Revocation
  - No direct interaction of some devices with KDC
- No time on device
  - Checking expiry
- Supporting sleepy nodes
  - AT-R only in the first message
- Enable instant start after power failure
  - Non-Volatile Memory needs to last 20 years
- Small isolated networks (which may later be part of a large networks)
  - Where should the KDC be located and transfer of responsibility
- Multicast communication patterns and effect on authorization
  - Who is the resource server and client