Feasibility of DTLS *for* the Internet of Things (IoTs)

Securing the IP-based Internet of Things with DTLS

draft-keoh-lwig-dtls-iot

***Sye Loong Keoh**, Sandeep S. Kumar, Oscar Garcia-Morchon*

IETF86 Mar 10 – 15, 2013, Orlando

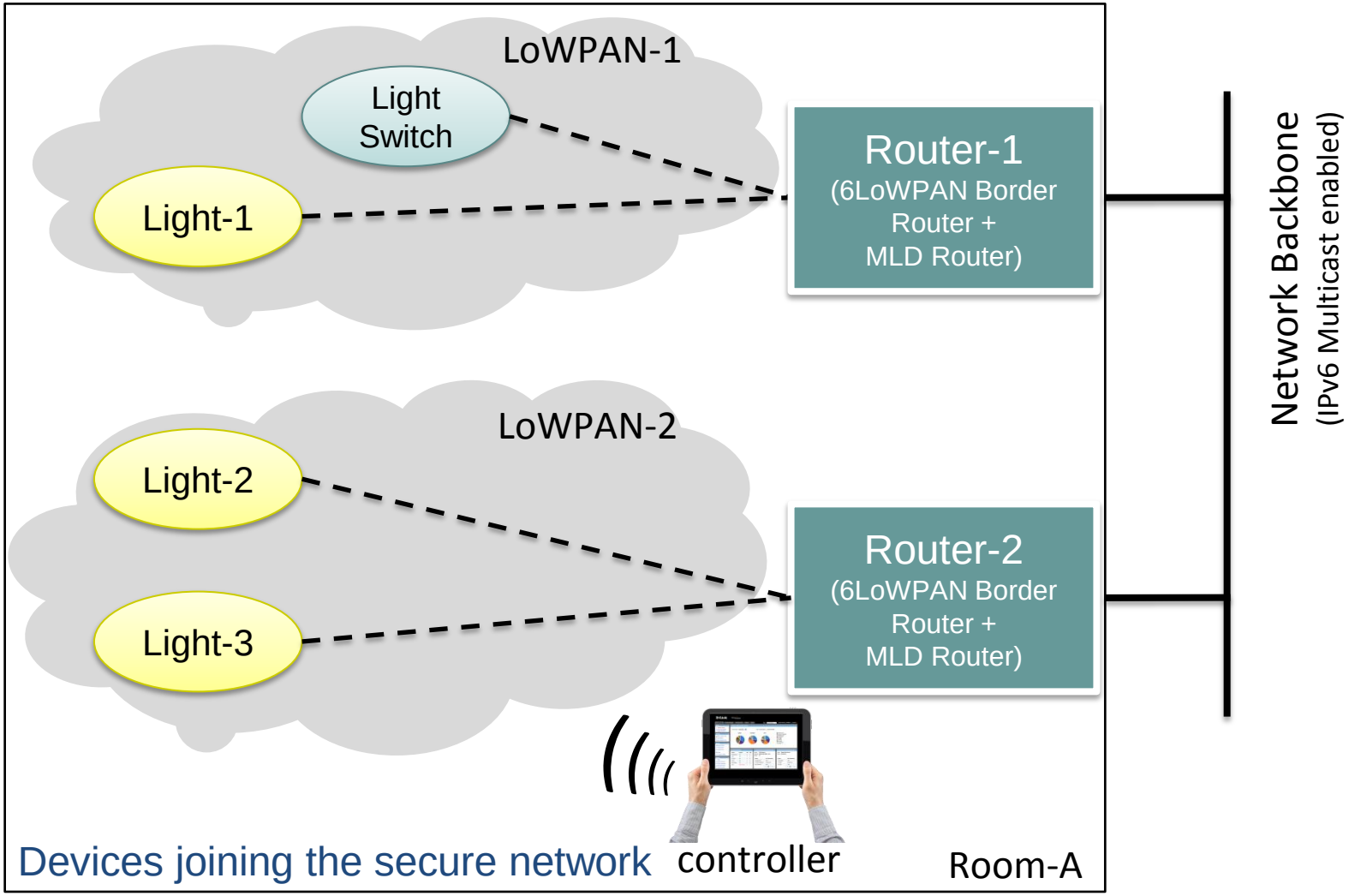
email: sye.loong.keoh AT philips.com

Motivation and Objectives

- There are many Internet security protocols, e.g., IPSec, IKE, (D)TLS, HIP, PANA, EAP, etc.
- Internet of Things (IoT) comprises many resource constrained devices.
- [Question] How to enable security functionalities for Machine-to-Machine (M2M) communication in IoT?
  - *Network access*: authentication of joining devices.
  - *Key management*: secure and authenticated channel.
  - *Secure unicast and multicast*: confidentiality and authenticity of application data.

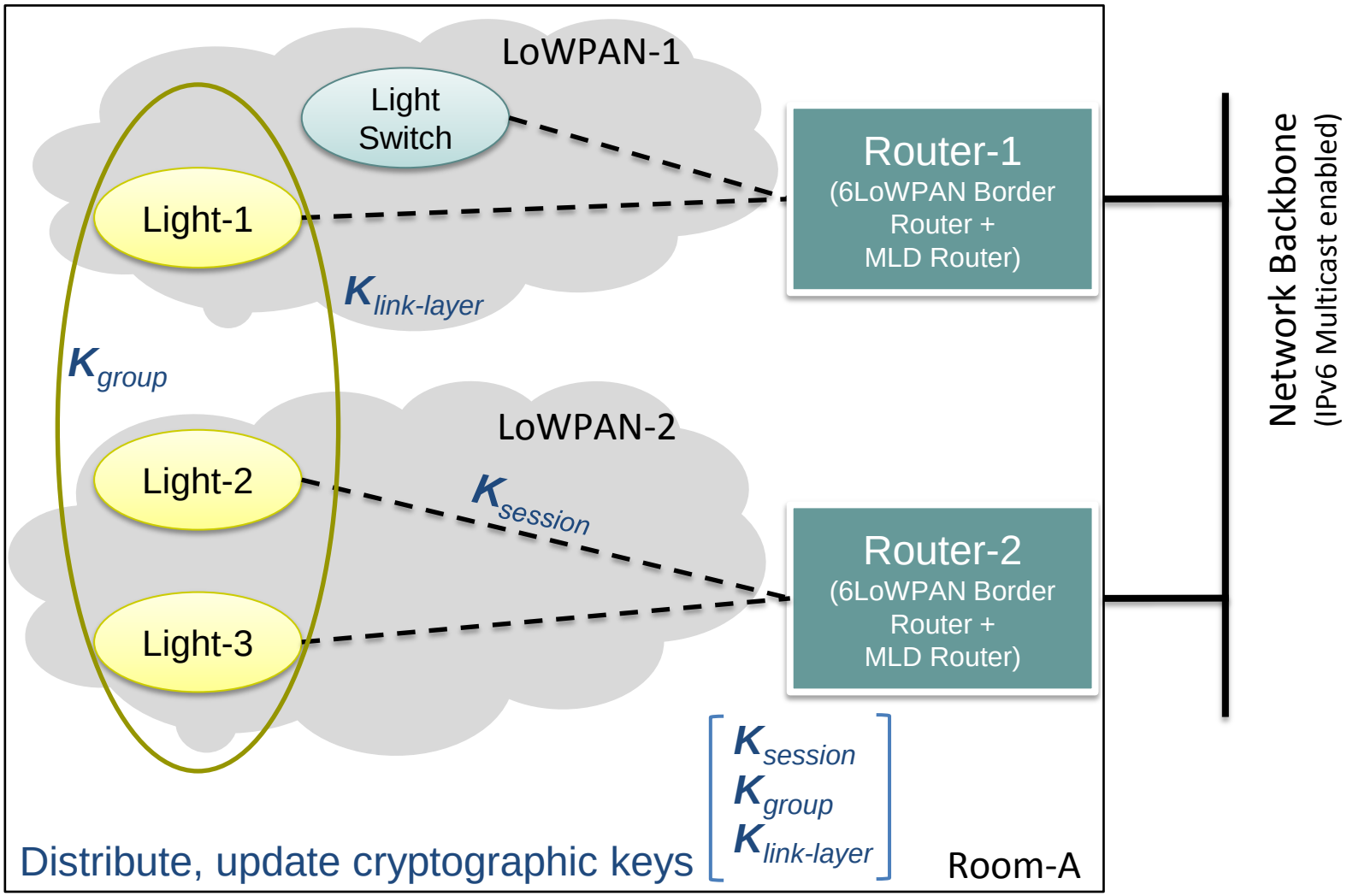
DTLS is **must-implement** for CoAP, this Internet Draft investigates the feasibility of using DTLS to achieve the required security functionalities.

DTLS Usage (1): Network Access



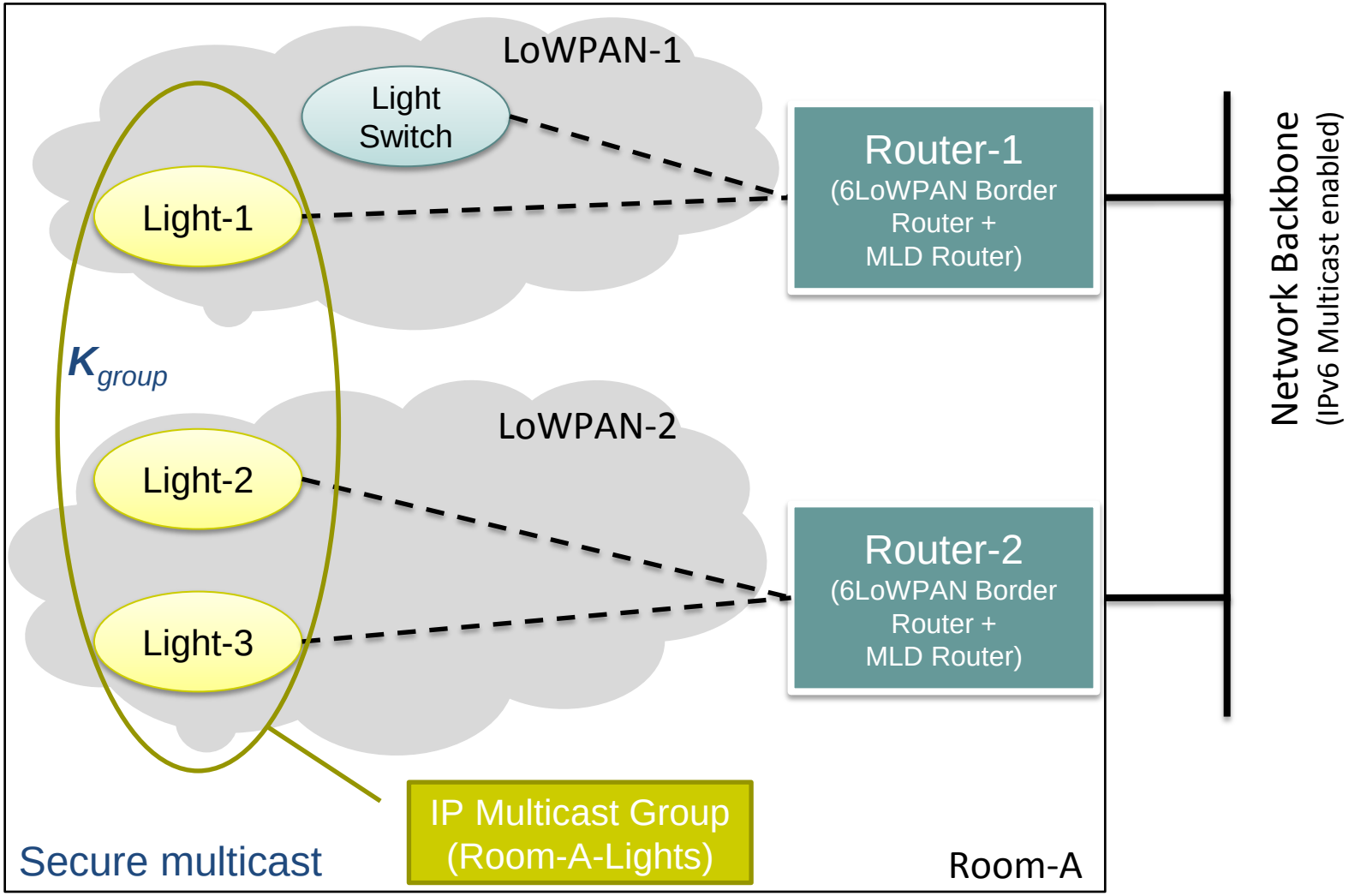
Adapted from Group Communication for CoAP

DTLS Usage (2): Key Management



Adapted from Group Communication for CoAP

DTLS Usage (3): Group Communication

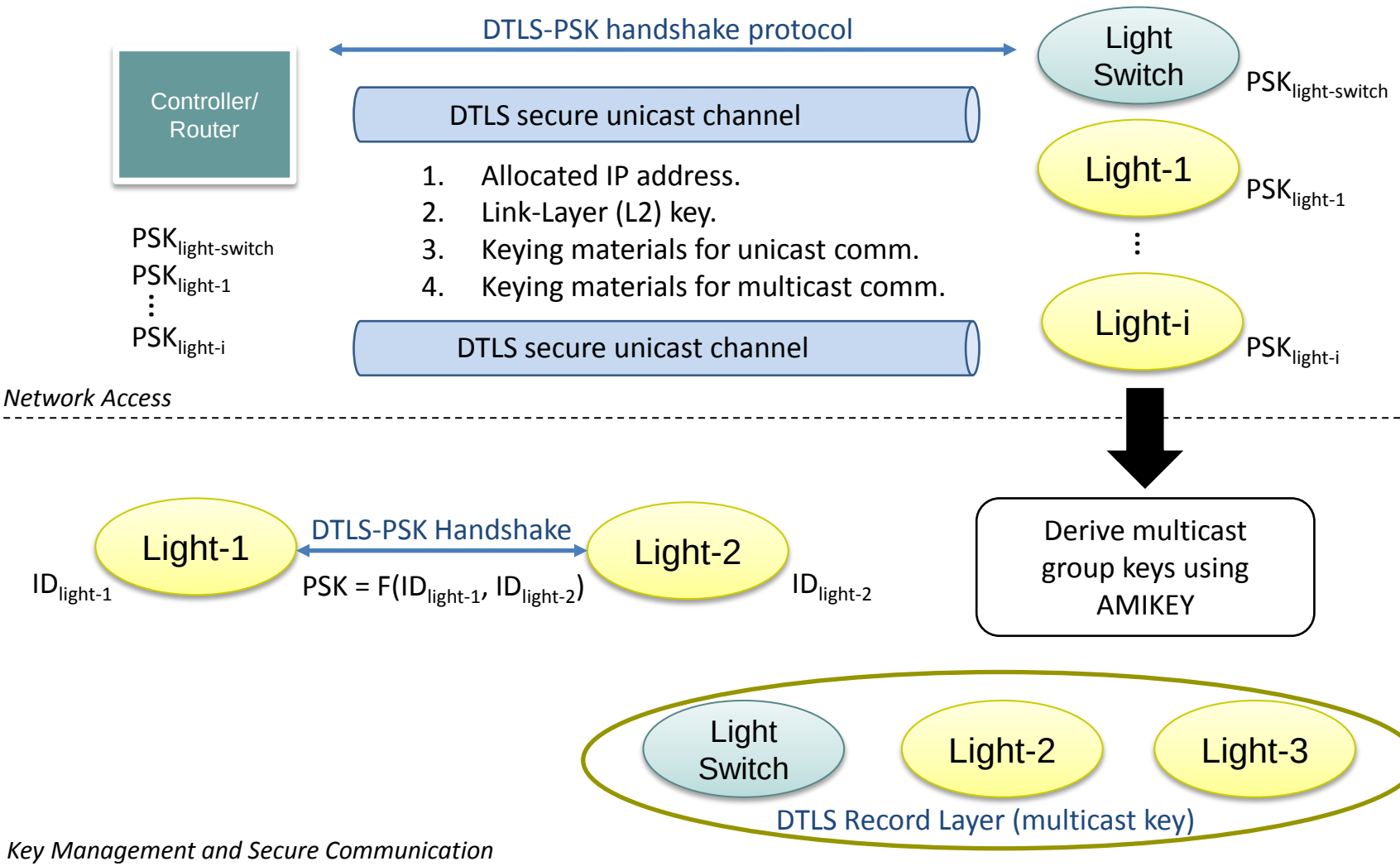


Source: Group Communication for CoAP

Assumptions

- Multi-hop wireless mesh network.
- Each device has been configured with a PSK during the manufacturing process.
- Network is protected with a *Link-Layer (L2) Key.*
- DTLS handshake protocol with *Pre-Shared Key (PSK)* mode is used.
- AMIKEY for multicast key management is used.

Overview


DTLS-PSK handshake protocol
Controller/ Router
DTLS secure unicast channel
1. Allocated IP address.
2. Link-Layer (L2) key.
3. Keying materials for unicast comm.
4. Keying materials for multicast comm.
DTLS secure unicast channel
Light Switch
PSK light-switch
Light-1
PSK light-1
Light-i
PSK light-i
PSK light-switch
PSK light-1
PSK light-i
Network Access
Light-1
ID light-1
DTLS-PSK Handshake
PSK = F(ID light-1, ID light-2)
Light-2
ID light-2
Derive multicast group keys using AMIKEY
Light Switch
Light-2
Light-3
DTLS Record Layer (multicast key)
Key Management and Secure Communication

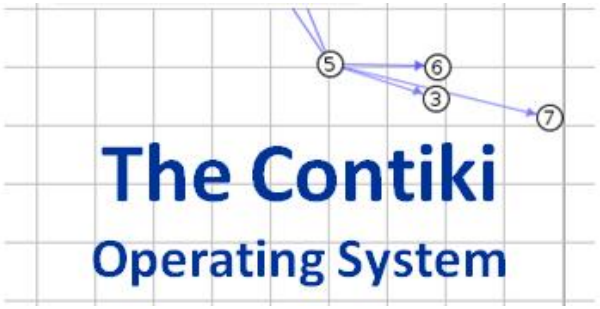
Implementation

Hardware Platform & Development Environment

- RedBee Econotag: 32-bit CPU, 128 KB (ROM), 128 KB (RAM), AES co-processor, 802.15.4 radio.
- Contiki OS 2.5, 6LoWPAN stack, TinyDTLS library

Modifications to the TinyDTLS

- Cookie mechanism is disabled.
- Separate message delivery instead of flight grouping of messages.
- New re-transmission and re-ordering mechanisms.
- AES library to use hardware co-processor.
- Added functionalities for key management.



Evaluation (1)

Memory Consumption

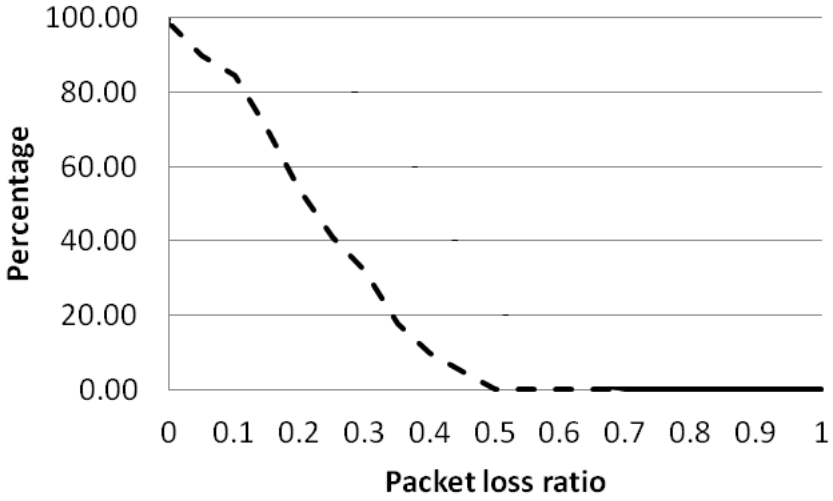
	DTLS	
	ROM (KB)	RAM (KB)
DTLS Handshake	8.15	1.9
Cryptography	3.3	1.5
Key Management	1	~0
Tx Multicast Msg	3.7	0.5
TOTAL	16.15	3.9

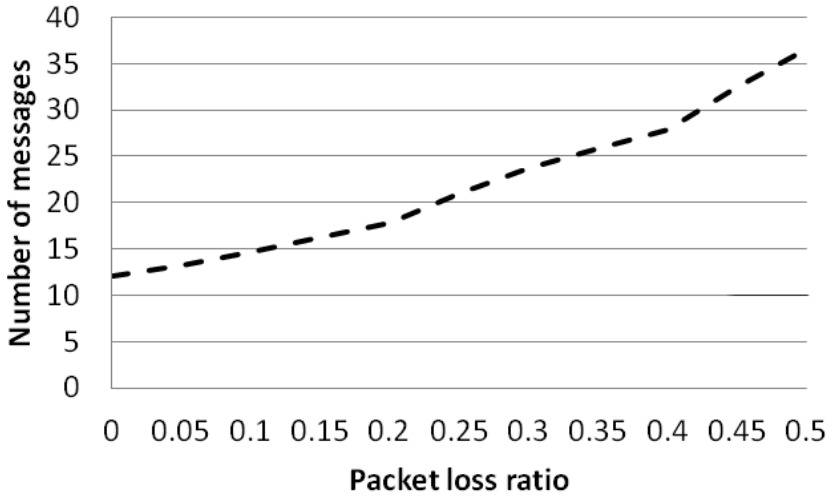
Communication Overhead

	DTLS
No. of Messages	12
No. of Round trips	4
802.15.4 headers	168 B
6LoWPAN headers	480 B
UDP headers	96 B
Application	487 B
TOTAL	1,231 B

- Large memory footprint in ROM and RAM.
  - Complexity of the DTLS handshake, i.e., many messages and states.
  - Crypto suites require SHA-2 that is not available on hardware crypto co-processor.
- Overhead due to lower layer per-packet protocol headers.

Evaluation (2)





- Higher packet loss ratio results in a failure probability of completing the handshake.
- When the packet loss ratio is 0.5, no DTLS handshake was successful.

- Delay in completing a DTLS handshake increases significantly if there is a packet loss.
- Lost packets must be re-transmitted, hence the number of messages also increases.

Conclusions

- Showed the very first step in attempting to use DTLS for secure *network access, key management and secure communication*.

- DTLS's handshake is still considered very complex, and hence optimization is still required.
  - Replace SHA-2 with AES-CMAC?
  - Investigate the feasibility of DTLS with raw public-key?

- Questions to the WG:
  - Do you think this is a valuable implementation experience to be documented?
  - Who is interested in contributing to this I-D?
  - Can we work towards a WG document?

Thank you