A Hitchhiker's Guide to the (D)TLS Protocol for Smart Objects and Constrained Networks

draft-tschofenig-lwig-tls-minimal

*Hannes Tschofenig, **Sandeep S. Kumar**, Sye Loong Keoh*

IETF87 Jul 28 – 2, 2013, Berlin

email: sandeep.kumar AT philips.com

Snapshot

TLS (Transport Layer Security) for securing over TCP connections

- suitable for HTTP

DTLS (Datagram TLS) for securing over UDP connections

- suitable for COAP

draft-tschofenig-lwig-tls-minimal-03 is

merge of **draft-keoh-lwig-dtls-iot-01**

- deleting network access and group communication

with **draft-tschofenig-lwig-tls-minimal-02**

- with additional TLS implementation details

Aim: Create a single document with all (D)TLS implementation guidance

(D)TLS implementations

Different modes

- Pre-shared keys
- Raw public-keys
- Certificates

I-D contains

- Design decisions guidance

- Implementation details for
    - DTLS in PSK mode -> memory, network performance
    - TLS in raw PK and certificate mode -> memory

Implementation 1: DTLS-PSK

Hardware Platform & Development Environment

- RedBee Econotag: 32-bit CPU, 128 KB (ROM), 96 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.

The Contiki
Operating System

Evaluation (1)

Memory Consumption

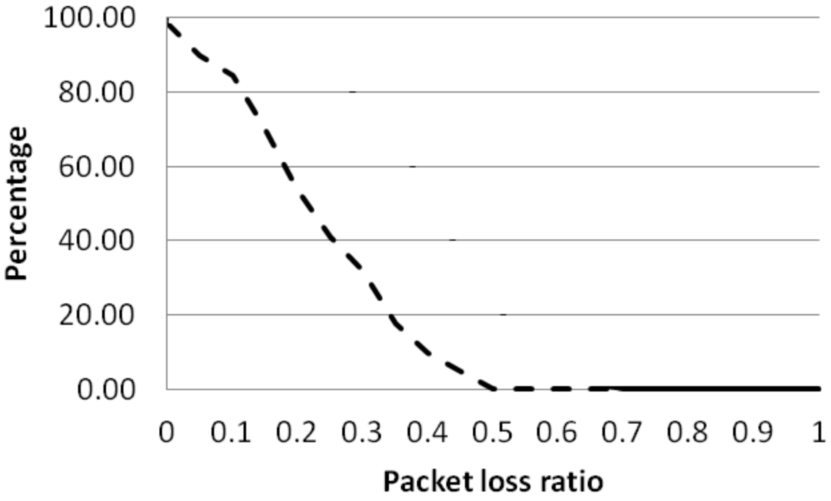
	DTLS	
	ROM (KB)	RAM (KB)
DTLS Handshake State machine	8.15	1.9
Cryptography	3.3	1.5
DTLS Record layer	3.7	0.5
TOTAL	15.15	3.9

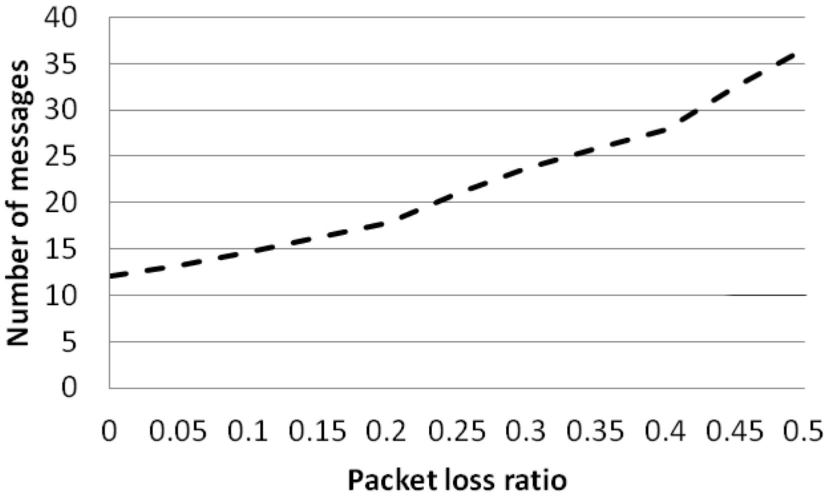
Communication Overhead

	DTLS
No. of Messages	8
No. of Round trips	2
802.15.4 headers	112 B
6LoWPAN headers	320 B
UDP headers	64 B
TOTAL	496 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.

Implementation 2: TLS cert and raw PK

- Certificate based and Raw-public key based TLS implementation
- Based on a modified version of the axTLS embedded SSL implementation

Evaluation – Crypto code

Code-size for cryptographic functions

Cryptographic functions	Code size
MD5	4,856 bytes
SHA1	2,432 bytes
HMAC	2,928 bytes
RSA	3,984 bytes
Big Integer Implementation	8,328 bytes
AES	7,096 bytes
RC4	1,496 bytes
Random Number Generator	4,840 bytes

Evaluation – Cert / Raw PK

Code-size for certificate based

Functions	Code size
x509 related	2,776 bytes
Certificate Processing Functions	4,456 bytes
ASN1 Parser	5,512 bytes
Generic TLS Library	15,928 bytes
TLS Client Library	4,584 bytes
OS Wrapper Functions	*2,776 bytes*
OpenSSL Wrapper Functions	*931 bytes*

Code-size for raw PK based

Functions	Code size
Minimal ASN1 Parser	3,232 bytes
Generic TLS Library	16,288 bytes
TLS Client Library	4,528 bytes
OS Wrapper Functions	*2,776 bytes*
OpenSSL Wrapper Functions	*931 bytes*

- Raw public key based does not require X.509 and certificate processing
- Smaller ASN.1 parser for only parsing header preamble in the *SubjectPublicKeyInfo* block.
- TLS library larger due to additional functionality added to load keys

Open issues

- Need more implementation experiences on "constrained" devices
  - In different scenarios requiring different choices
  - With other relevant (D)TLS defined extensions
  - Long-lived vs Resume sessions
  - Fragmentation during handshake
  - With network performance measurement in LLN
- If you have data and would like to contribute please contact us.

DICE BoF

- DTLS for Constrained Environments (DICE) BoF
  - A minimal configuration profile of DTLS for IoT
  - Group communication security supported by DTLS Record Layer

- This work will continue to provide implementation experiences and guidance to DICE