Bounds for the Scalability of TLS over LoRaWAN

26. ITG Fachtagung Mobilkommunikation - Technologien und Anwendungen

Michael Rademacher[1], Hendrik Linka[2], Jannis Konrad[2], Thorsten Horstmann[1,2], Karl Jonas[2]

[1] Fraunhofer FKIE
Cyber Analysis and Defense
Bonn, Germany

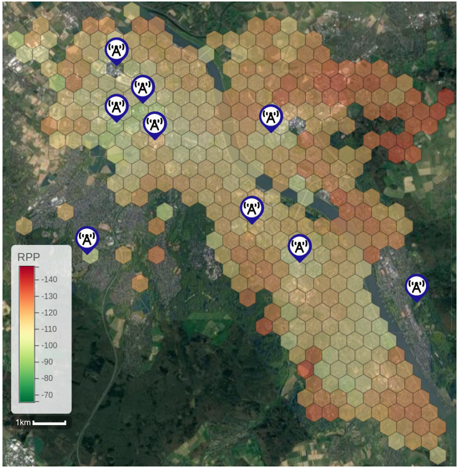
Fraunhofer
FKIE

[2] University of Applied Sciences Bonn-Rhein-Sieg
Computer Science
Sankt Augustin, Germany

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

18.05.2022, Osnabrück

Motivation: Digitize public infrastructure i.e. Smart Metering



M. Rademacher et al., "**Path Loss in Urban LoRa Networks: A Large-Scale Measurement Study**" in 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall) [3]

- **Reliable** and **secure** communication is needed for smart city applications
- low-power wide-area networks (LPWANs):
  - licensed bands (NB-IoT, LTE-M, 5G mMTC)
  - license-exempt bands (**LoRaWAN** or SIGFOX)
- Scalability of **LoRaWAN** in license-exempt bands:
  - Interference
  - **Duty cycle limitations**

Why and Why not LoRaWAN AND TLS? (2)

1. TLS has become the standard for end-to-end secured communication.
2. There exists known vulnerabilities/attacks for LoRaWAN.
3. In **critical domains** (i.e. smart metering) TLS is a **mandatory requirement**. [1]

Technische Richtlinie BSI TR-03116
Kryptographische Vorgaben für Projekte der Bundesregierung

Teil 3: Intelligente Messsysteme

→ Kommunikationspartner im WAN MÜSSEN eine TLS-Session (inklusive eventueller Session Resumptions) auf einen Wert begrenzen, der 48 Stunden nicht überschreitet. Beim Smart Meter Gateway SOLLTE dieser Wert durch den Gateway Administrator konfigurierbar sein. Insbesondere MUSS das Smart Meter Gateway bestehende TLS-Verbindungen nach Ablauf dieser Zeit beenden und für eine neue Verbindung einen neuen TLS-Handshake durchführen.

1. Increased battery usage due to cryptographic operations.
2. Certificate handling.
3. **Protocol overhead** in combination with **duty cycle limitations** per band.

Duty-cycle and EIRP in the EU [4]

Which upper bounds (scalability) exists for or the usage of TLS and LoRaWAN?

Scenario:

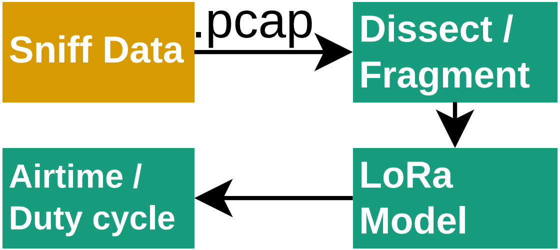
- **IP - TCP/UDP - TLS** is encapsulated as LoRaWAN Payload [5, 6]
  - Fragmentation at 250 Byte with 13 Byte Header LoRa Header.
- Focus on **full, mutual TLS handshakes** with 10 Byte data.

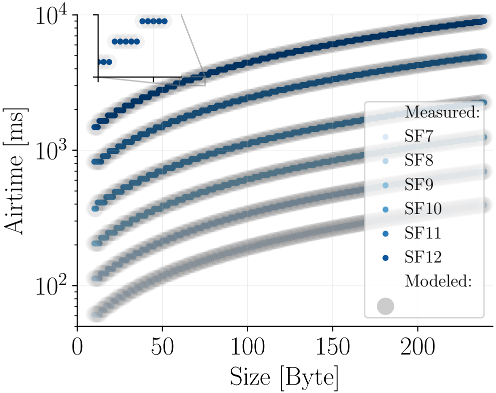
Assumptions:

- A wireless link is symmetric: the SF for the uplink and for the downlink is identical.
- There are no lost transmissions, neither due to collisions nor interference.
- The medium access is perfectly distributed (best usage of duty cycle).
- Uplink: a sensor uses a single band with a duty cycle limit of 1 %.
- Downlink: the gateway uses a band with 10 % duty cycle and a band with 1 % duty cycle.

Method: A tool to calculate the airtimes and relate these to duty cycle limits.

LoRa airtime modeling tool.





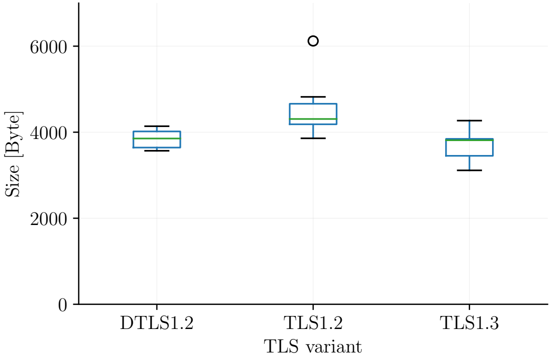
- Verification using an external SDR leads to marginal errors ($<< 1\%$.)
- All data, plots and the LoRa airtime modeling tool is **publicly available on github** [2].

Evaluated TLS versions and cipher suites.

Cipher suites marked with ✕ are part of the security concept presented in [1] and cipher suites marked with ❍ are added by us. The smallest and largest ciphers suites are marked with (S) and (L).

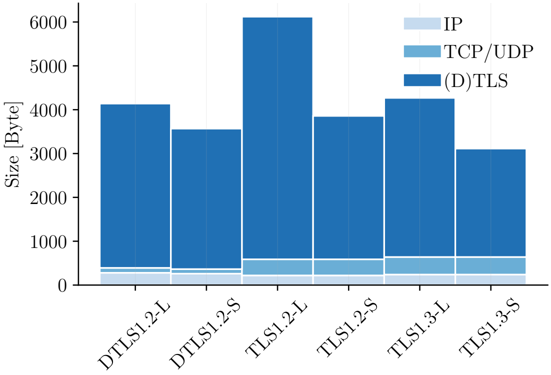
Version	Cipher Suites	Elliptic curve						RSA
		secp256r1	secp384r1	brainpoolP256r1	brainpoolP384r1	brainpoolP512r1	ED25519	2048
TLS1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	✕(S)		✕	✕			
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		✕		✕	✕		
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256		✕		✕	✕		
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384		✕		✕	✕		
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384							❍(L)
TLS1.3	TLS_AES_128_GCM_SHA256	✕	✕	✕	✕	✕	❍(S)	
	TLS_AES_256_GCM_SHA384	✕	✕	✕	✕	✕(L)	❍	
	TLS_AES_128_CCM_SHA256	✕	✕	✕	✕	✕		
DTLS1.2	DTLS12_ECDHE-ECDSA-AES128-GCM-SHA256	❍(S)	❍					
	DTLS12_ECDHE-ECDSA-AES256-GCM-SHA384	❍	❍(L)					
	DTLS12_ECDHE-ECDSA-AES128-CBC-SHA256	❍	❍					
	DTLS12_ECDHE-ECDSA-AES256-GCM-SHA384	❍	❍					

TLS versions and cipher suite handshake size comparison. (6)



Transmission size of TLS handshakes for up- and downlink combined.

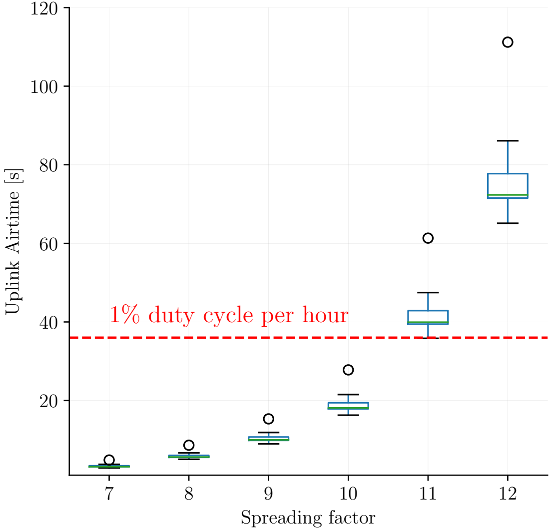
- DTLS is not beneficial for handshake sizes.
- DHE with RSA is considerably larger



Cipher suites transmission sizes grouped by layer.

- The vast majority of data in the handshake is TLS itself, in particular, the certificates.

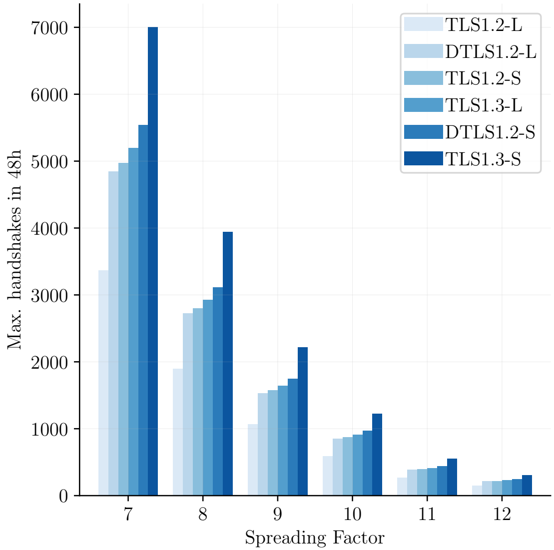
Consumed Airtime in the uplink for different SFs.



Each sensor uses a single band with a duty cycle limit of 1%:

- The airtime stays well below the desired limit of two days.
- In the uplink, the requirements in [1] can be fulfilled.
- For SF 11 and SF 12 the handshake will take more than 1 h which is the observation period for a duty cycle [4].

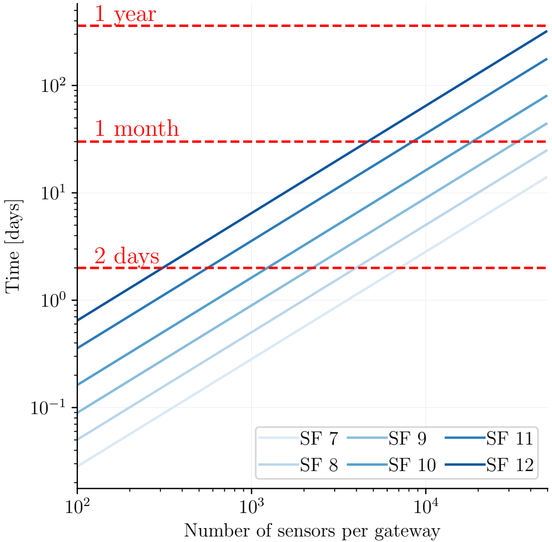
Maximum number of TLS handshakes in the downlink in 48h



Downlink: the gateway uses a band with 10% duty cycle and a band with 1% duty cycle.

- More complex since a gateway is connected in a 1:n relationship to sensors.
- The range to fullfill the requirements in [1] is significant.
  - Factor 2 between the smallest and largest cipher suite (all SF).
  - Factor 7 between the SF.
- **Upper Bound: SF7 and TLS1.3-S = 7000 handshakes every two days**

Minimum time-span between two handshakes using TLS1.3-S.



- **50.000 sensors per gateway:**
  - All SF: a handshake once a year.
  - SF 7 and 8: a handshake once a month.

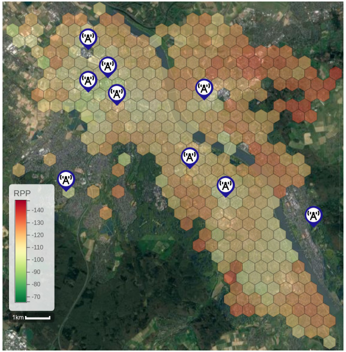
Summary and future work

- Developed and published [2] **a tool to assess upper bounds for duty cycle limitations** in LoRa Networks **for arbitrary traffic pattern.**
- **Evaluated the upper bounds for TLS and LoRaWAN**, in particular, the requirements for smart metering in Germany [1]:
- Bottleneck is the gateway: **Upper bound** of 7000 TLS handshakes every two days.

However, this work assumes:

1. No lost transmission (collisions, interference) → **Simulation?**
   - Hypothesis: A significant reduction for possible handshakes.
2. No additional data → **realistic traffic pattern?**
   - Hypothesis: DTLS is superior compared to TLS
3. Uniform SF per gateway → **realistic distribution for the SFs**
   - Orthogonal SFs vs. Airtime?

Source Code of this work:
https://github.com/mclab-hbrs/lora-tls
Source Code propagation modeling:
https://github.com/mclab-hbrs/lora-bonn



Bibliography

BSI.
Kryptographische Vorgaben für Projekte der Bundesregierung - Teil 3: Intelligente Messsysteme, 2020.

Michael Rademacher.
Code for this work.
https://github.com/mclab-hbrs/lora-tls.

Michael Rademacher, Hendrik Linka, Thorsten Horstmann, and Martin Henze.
Path loss in urban lora networks: A large-scale measurement study.
In *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, pages 1–6, 2021.

Martijn Saelens, Jeroen Hoebeke, Adnan Shahid, and Eli De Poorter.
Impact of eu duty cycle and transmission power limitations for sub-ghz lpwan srds: An overview and future challenges.
EURASIP J. Wirel. Commun. Netw., 2019(1):1–32, dec 2019.

Shie-Yuan Wang and Chia-Hung Chang.
Supporting tcp-based remote managements of lora/lorawan devices.
In *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, pages 1–5, 2019.

Patrick Weber, Daniel Jäckle, David Rahusen, and Axel Sikora.
Ipv6 over lorawan™.
In *2016 3rd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, pages 75–79, 2016.