Bounds for the Scalability of TLS over LoRaWAN

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

[1]*Fraunhofer FKIE, Cyber Analysis and Defense, Bonn, Germany*
[2]*University of Applied Sciences Bonn-Rhein-Sieg, Sankt Augustin, Germany*

***Abstract*—Reliable and secure communication is needed to further digitize public infrastructure. LPWANs operating in license-exempt bands are a promising candidate. This work address the concept of a secure LPWAN by evaluating TLS over LoRaWAN. The overhead induced by TLS in combination with the duty cycle restrictions make this combination challenging. In this work, upper bounds of the usage are compiled by estimating the number of full TLS handshakes under various conditions. An airtime model is verified and integrated into a tool to estimate possible bounds on the duty cycle. The results reveal that a bottleneck exist in the downlink which depends on the Spreading Factor of LoRa and the selected cipher suite.**

***Index Terms*—LoRa; LoRaWAN; Security; Scalability; TLS**

I. Introduction and Motivation

The digitization of public infrastructure is becoming reality. Reliable and secure communication is needed to collect data from various facilities and components. Based on the collected data, an infrastructure operator can remotely react to certain events to realize new digital applications or to spare manual and labor-intensive monitoring of already deployed infrastructure. Where fixed-line networks are unavailable or not feasible wireless networks are used instead. A promising class of wireless networks are low-power wide-area networks (LPWANs) either operating in licensed bands (Narrowband Internet of Things (NB-IoT), LTE-M, 5G Massive Machine Type Communication (mMTC)) or license-exempt bands (Long Range Wide Area Network (LoRaWAN) or SIGFOX) [1].

One example of infrastructure which can benefit from LPWANs are smart energy grids to handle more complex tasks efficiently. However, a long-lasting blackout can have a severe impact in a modern society and therefore energy grids are considered one of the most worth protecting critical infrastructures. A well-defined security concept for LPWANs operating in this domain is therefore indispensable. In Germany, such a concept is provided by the Federal Office for Information Security (BSI) in a technical guideline for all smart metering applications [2].

In this work, we address the concept of a secure LPWAN by evaluating the combination of LoRaWAN and Transport Layer Security (TLS). LoRaWAN operates in a license-exempt band which reduces the operational expenditure (OPEX) significantly. In addition, real-world experiments show that battery-powered LoRaWAN devices can communicate over long-distances in urban and sub-urban areas [3], [4].

TLS has become the standard for end-to-end secured communication. Due to the widespread and the well investigated security mechanism it is often regarded as a *mandatory requirement* in different security concepts such as the one for smart metering applications in Germany [2]. However, since TLS is not designed for constrained devices and networks, the combination of LoRaWAN and TLS imposes several challenges. Among others, the main challenges are the increased battery usage, the certificate handling and the protocol overhead. This work mainly deals with the latter. Since regulatory restrictions in the license-exempt band limit the amount of time each device is allowed to send data (duty cycle), the overhead of TLS can limit the applicability for LPWANs. The main contributions of this work are:

- This work experimentally verifies airtime calculations using real-world Long Range (LoRa) transceivers by implementing a framework which is capable of sending arbitrary data (i.e. IP, TCP and TLS) over LoRa.
- This work discusses and derives upper bounds (best-cases) due to duty cycle limitations for the scalability of using TLS in combination with LoRaWAN based on the requirements in [2].

The rest of this work is structured as follows: Section II provides the reader with a short background on LoRaWAN and TLS. Afterwards, we provide a summary of related work in Section III. An extended methodology is provided in Section IV to guarantee soundness of the results. In addition, the code and data has been made publicly available [5]. Section V presents the main results and in Section VI we shortly conclude our findings.

II. Background

In this section we provide a short introduction for LoRaWAN and TLS. A detailed description is due to space limitations not feasible; however, a plethora of great material exists, and we refer the reader to those.

A. LoRaWAN

LoRa is a wireless communication technique to transmit small payloads over large distances. The most common frequency bands for LoRa are $433\,\mathrm{MHz}$ and $868\,\mathrm{MHz}$ while the latter is mainly used in Europe. Regulatory restrictions are in place that limit the amount of time a transceiver is allowed to send per hour (duty cycle). For different sub-bands, varying duty cycles apply.

In general the duty cycle in Europe is set fixed to $1\,\%$ ($863.0\,\mathrm{MHz}$ to $868.6\,\mathrm{MHz}$, $869.7\,\mathrm{MHz}$ to $870.0\,\mathrm{MHz}$) with two exception where it is set to $0.1\,\%$ ($868.7\,\mathrm{MHz}$ to $869.2\,\mathrm{MHz}$) and $10\,\%$ ($869.4\,\mathrm{MHz}$ to $869.65\,\mathrm{MHz}$) [6]. The

duty cycle is applied to each transmitting device individually, however, a device can use multiple bands sequentially.

LoRa uses a spread spectrum modulation technique patented by the company Semtech [7]. This proprietary modulation builds upon the general idea of Chirp Spread Spectrum (CSS). By utilizing the entire allocated bandwidth for a transmission, CSS is more resistant to interference and multi-path fading compared to traditional modulation schemes used in cellular networks. The most important parameters for the physical layer of LoRa are the bandwidth, the Spreading Factor (SF) and the Code Rate (CR). The SF determines the number of raw bits that can be encoded by transmitting a symbol. In addition, it directly influences the symbol duration. The data rate approximately doubles by either decreasing the SF step-wise or by doubling the bandwidth. A comprehensive description of the modulation technique is provided in [8]. In general, the data rate of a LoRa transmission is limited compared to other wireless communication techniques and the duty cycle imposes an additional challenge especially with further overhead due to security mechanisms.

The term LoRa only refers to physical layer mechanisms. By far the most common protocol for the upper layers is called LoRaWAN — an open specification developed and maintained by the LoRa Alliance [9]. The main purpose of the LoRaWAN is to define protocols to manage and route the communication between sensors and applications. Typical components in the hierarchy of these networks are sensors, gateways, a network server and application servers. A sensor gathers data which is transmitted to one or multiple gateways via LoRa. LoRa offers a maximum packet size of 256 B [10]. A gateway simply decodes and afterwards forwards it to a network server using an arbitrary backhaul technology. The network server implements the main functions and services of LoRaWAN. Common tasks are security checks, dynamic adoption of the SF or handling of redundant packages. The network server afterwards encapsulates the messages and forwards it to the final destination called application server. A typical LoRaWAN topology can be described as several interconnected stars with a gateway as the center of a star. The duty cycle limitations apply to the gateways and the sensors [6].

LoRaWAN networks employ two different layers of security. The first is located between sensors and the network server to ensure the authenticity of the devices. The second layer is an encryption between the sensor and the application server. The application server needs to be trusted since it encrypts and decrypts the LoRaWAN payload. The exchange of the required key material, for both layers, is one of the main security challenges. A description of the LoRaWAN architecture is available in [12] and [13] describes the security mechanism in detail.

B. Transport Layer Security

The TLS protocol is used to provide a secure communication channel between two applications. In more detail, the goal is to provide encryption (privacy), authentication and data integrity over an insecure medium between two parties who have never met before [14]. TLS operates on top of Transmission Control Protocol (TCP) and all data exchanged within a TLS session is framed using the so-called TLS record protocol [14].

To establish a secure connection, TLS uses a handshake protocol to provide authentication using digital certificates (X509) and to agree on cipher suites and a master secret. The handshake protocol is the most complex part of TLS making use of several message types to securely exchange the desired key material. In a traditional TLS handshake, for example when accessing a website with a web-browser, the server transmits a certificate to the client which the client uses to authenticate the server. However, the server does not authenticate the client. While this one-way authentication is useful in the context of the Internet, for secure Internet of Things (IoT) infrastructures, a mutual authentication is often desired. By transmitting a client certificate to the server, it is possible to restrict and block connections from unauthorized clients to the server infrastructure. TLS can be used with a variety of different so-called cipher suites which defines the set of algorithms used to secure the connection. A cipher suite is the combination of a key exchange (e.g. Elliptic-Curve Diffie–Hellman (ECDH)), authentication (e.g. Elliptic Curve Digital Signature Algorithm (ECDSA)), encryption (Advanced Encryption Standard (AES)) and a message authentication (Secure Hash Algorithm (SHA)) algorithm.

Emerging from its initial name SSL, the TLS-protocol has been undergoing various different versions. Currently, TLS 1.2 [14] and TLS 1.3 [15] are preliminary in use. The recent version TLS 1.3 improves the efficiency and addresses several weaknesses identified in TLS 1.2 [16]. The main goals of TLS 1.3 compared to its predecessor are the improved security with modern cryptographic functions, the encryption of more messages used in the handshake protocol and an increased performance by using 1-RTT and 0-RTT handshakes.

The Datagram Transport Layer Security (DTLS)-protocol [17] is intended to provide similar security features as TLS with the crucial difference that it uses User Datagram Protocol (UDP) as a transport layer protocol. Since the TLS-handshake protocol relies on a defined packet order but UDP has no mechanisms for retransmissions and reordering of packets, the DTLS-protocol implements these mechanisms. To deal with packet loss, DTLS uses a simple retransmission timer and to account for reordering an additional 8 B sequence number is added to the handshake messages. DTLS only relies on block ciphers since stream ciphers, such as RC4 used in TLS 1.2, are prone to vulnerabilities with lost and reordered packets.

III. Related Work

Encapsulating common protocols in LoRaWAN (i.e. IPv6 or TCP) has been addressed beforehand [11], [18]. Common challenges are the overhead due to the additional headers, significantly different Maximum Transmission Units (MTUs), handling of re-transmissions and timeouts of protocol states.

Different solutions have been proposed like IPv6 header compression, additional fragmentation and adaption of protocol parameters (e.g. TCP Retransmission Timeout (RTO)).

The security mechanism of LoRaWAN have been evaluated by different researchers. The authors in [13], [19], [20] provide a detailed overview of known vulnerabilities of the built-in mechanism. Many of these vulnerabilities have been already addressed in the most recent LoRaWAN specification. However, new vulnerabilities recently emerged. The authors in [21] propose a distributed LoRa transmitter network in combination with a centralized controller framework. Using this framework, the authors successfully introduce a novel denial-of-service (DoS) attack exploiting the adaptive data rate (ADR) techniques of LoRaWAN and experimentally validated a beacon spoofing attack.

The previous attacks, the fact that new attacks still emerge, and the possibility to secure data end-to-end drive the need for an additional layer of *payload security* in LoRaWAN networks. As already discussed, a well-known and often required solution is TLS. In the following, we focus on previous work dealing with LoRaWAN and TLS.

The authors in [22] propose a new protocol for end-to-end encryption with perfect forward secrecy in LoRaWAN networks. To benchmark their new approach, the authors compare it to DTLS-Elliptic Curve Cryptography (ECC) and DTLS-Pre-shared key (PSK) in a numerical simulation. By summing up the packet sizes of the different messages in the DTLS protocol, the authors describe that the overhead of using DTLS-ECC is 746 B and the overhead of using DTLS-PSK is 198 B. However, there is no direct description of the impact of this overhead to a LoRaWAN transmission.

The authors in [23] focus on the key exchange by comparing DTLS and Ephemeral Diffie-Hellman Over COSE (EDHOC) [24] as an alternative to the built-in LoRaWAN procedures. The authors provide a detailed list of the frame sizes in the key exchange of both protocols and describe that EDHOC key exchange uses 40% less data compared to DTLS. In addition, they calculated the airtime for all messages of the EDHOC protocol. The results show that for most SFs, the airtime will violate European radio-band restrictions, hence a fragmentation of the messages is needed.

The patent [25] deals with DTLS over LoRaWAN. The authors describe that using DTLS with LoRaWAN significantly outperforms TLS in terms of spectral efficiency due to the reduced packet header of UDP in comparison to TCP. In addition, an intermediate layer is added between the client/server applications and the LoRaWAN network to deal with fragmentation and timeout issues.

IV. Methodology

To evaluate the bounds of LoRa and TLS, we use a mathematical model to calculate the airtime and relate this airtime to the duty cycle limits. The mathematical airtime model has been verified with a Commercial Off-the-Shelf (COTS) LoRa transceiver. In addition, we have obtained the transmission size of TLS handshakes with different TLS variants and cipher suites. Instead of presenting the mathematical model in detail, we made all developments publicly available in a GitHub repository [5]. Therefore, we will only discuss the most important aspects in the following.

A. Airtime model

We build upon a public available LoRa airtime model written in Python [26] which we extended with the following features: A user can import a captured communication using the well-known pcap file format. The data in the pcap file is parsed and dissected to differentiate between protocols (IP, TCP, TLS). Afterwards, the data is fragmented to account for the maximum MTU of LoRa. We assume that all data is encapsulated as a payload of multiple LoRa fragments. Therefore, additional header information of LoRa are added to every fragment. The airtime is calculated individually for the uplink (i.e. from sensor to gateway) and downlink (i.e. from gateway to sensor). Further parameters like the SF and the bandwidth can be specified. Based on the consumed airtime, we estimate the number of possible bidirectional communications. In summary, the developed tool loads a pcap file and outputs the number of times this pcap file can be transmitted in a certain time period (e.g. every day) without violating the duty cycle limit of the involved LoRa sensor and LoRa gateway.

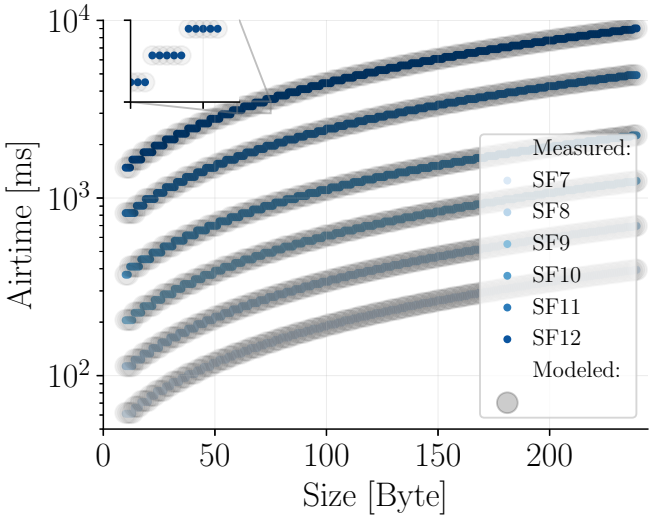

Fig. 1: Verification of the LoRa airtime model using measurements from an external Software Defined Radio (SDR).

To verify the airtime model used, we conducted a small experiment. We artificially generated LoRa payload data with a size of 10 B to 240 B in 1 B steps. The payload is transmitted using a COTS RFM95W LoRa modem. Using a HackRF SDR, which is sniffing in parallel on the same frequency, we obtained the raw airtime of a transmission. We conducted that experiment for all available SFs and for a bandwidth of 125 kHz. Afterwards, the airtime obtained with the SDR is compared with the mathematical model. The results are

TABLE I: Evaluated TLS versions and cipher suites. Cipher suites marked with ✕ are part of the security concept presented in [2] 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	❍	❍					

visualized in Figure 1 and demonstrate that the airtime model is able to estimate LoRa airtime without notable deviations.

B. TLS/DTLS handshake size

In this work, we are particularly interested in the combination of LoRaWAN and TLS to further secure communication in public infrastructures. As described in Section II-B, a key component of TLS is the handshake protocol. We are interested in mutual authentication where both server and client transmit a certificate as required by the security concept for smart metering applications in Germany [2]. In addition, for this work, we selected a subset of all possible cipher suites specified for TLS and DTLS. This subset is again based on [2] where only cipher suites with a certain security level are allowed. We added a few additional cipher suites due to the following reasons. First, the concept in [2] does not specify the usage of DTLS which we are interested in due to the usage of UDP as a transport protocol. Second, we added one cipher suite which uses a key exchange algorithm based on Rivest–Shamir–Adleman (RSA) instead of elliptic curve cryptography since RSA is still widely used. Third, we added ED25519 [27] as an emerging alternative to previous elliptic curves. Table I shows an overview of all TLS variants and cipher suites used.

To get the size and the message count for each cipher suite, a handshake and a $10\,\mathrm{B}$ payload is recorded with the tool "tshark" and the library "openssl". The resulting pcap files are analyzed with the airtime model. We made all pcap files available at [5].

C. Scenario and assumptions

We assume a typical urban LPWAN scenario where a local LoRaWAN network is used to connect multiple remote smart energy grid sensors. Since the goal of this work is to explore upper bounds for this scenario, we make the following assumptions:

- A wireless link is symmetric: the SF for the uplink and for the downlink is identical.
- All sensors at one gateway use the identical SF. Since we are interested in the influence of the SF, we do not incorporate any distribution function for SFs in this work.
- There are no lost transmissions, neither due to collisions nor interference.
- The medium access is perfectly distributed so that the duty cycle is used in the best possible way.
- In the uplink, a sensor uses a single band with a duty cycle limit of $1\,\%$.
- In the downlink, the gateway uses either a band with $10\,\%$ duty cycle or a band with $1\,\%$ duty cycle. This reflects the configuration that a gateway either responds on the same channel of an uplink transmission ($1\,\%$) or uses a default channel ($10\,\%$) [6].
- We are considering handshakes with a transmission of a $10\,\mathrm{B}$ payload without any additional transmission of data before the next handshake takes place. In particular, we do not model any traffic patterns by the sensors.

The combination of these assumptions reflects a best-case scenario which is solely focusing on the maximum number of possible handshakes.

The following analysis is driven by the defined scenario and the possibility to fulfill the mandatory requirements provided in [2]. Besides the usage of the specified cipher suites (cf. Table I) the most interesting aspect in [2] is, that it is mandatory, to conduct a full handshake after $48\,\mathrm{h}$ to re-establish a new TLS connection.

V. Results

This section is twofold. First, we provide general insights in the transmission sizes of TLS and DTLS handshakes, afterwards we consider duty cycle limitations in uplink and downlink individually.

Figure 2 visualizes the transmission sizes of handshakes. There is no significant difference between DTLS, TLS1.2 and TLS1.3. One notable outlier exists and corresponds to the usage of RSA in combination with TLS1.2 (TLS1.2-L in Table I). Most of the transmission is the TLS protocol itself, as Figure 3 reveals. Figure 3 shows the transmission size grouped by protocols (IP, TCP/UDP and (D)TLS) for six different cipher suites. These cipher suites correspond to the smallest (S) and largest (L) for DTLS, TLS1.2 and TLS1.3 (cf. Table I).

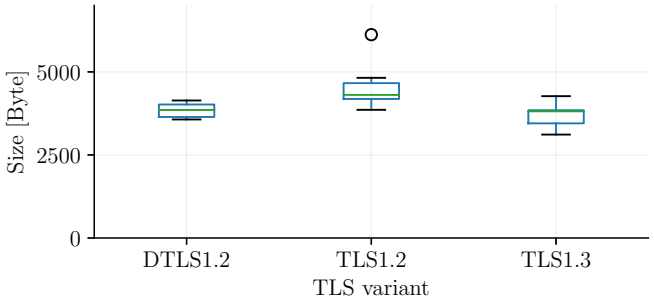

Fig. 2: Transmission size of TLS handshakes for up- and downlink combined.

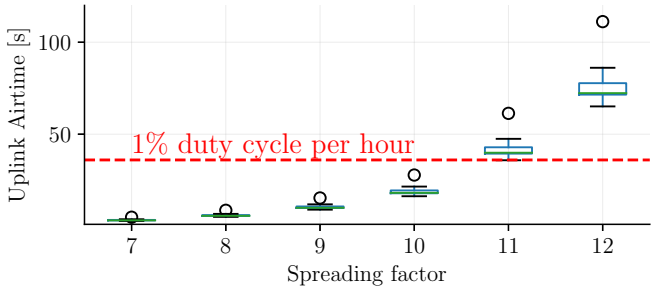

Fig. 4: Consumed Airtime in the uplink for different SFs. The airtime stays well below the desired limit of two days.

In the following, we will focus on the uplink (from an individual sensor to the gateway). Using the verified airtime model, we calculated the corresponding airtime in the uplink for all combinations of DTLS/TLS and cipher suites (cf. Table I). The results are visualized in Figure 4.

Notably, the consumed airtime increases with the SF used. The airtime ranges from 2.8 s for SF 7 in combination with the smallest cipher suite (TLS1.3-S) to 111.2 s for SF 12 and the largest cipher suite (TLS1.2-L). For all combinations of SFs and handshakes the consumed airtime is well below the duty cycle limit for two days (1762 s). This indicates, that in the uplink, the requirements in [2] can be fulfilled. However, it should be noted, that for SF 11 and SF 12 the handshake will take more than 1 h which is the observation period for a duty cycle [6]. If this leads to unwanted time-outs for the TLS protocol needs to be further discussed.

The duty cycle limitation in the downlink is more complex since a gateway is connected in a 1:n relationship to sensors. Instead of using a single sub-band with 1 % duty cycle, a gateway (mostly) operates on multiple channels and bands. In this analysis, we assume the combined usage of a band with 10 % duty cycle and with 1 % duty cycle.

Again, we are interested in the fulfillment of the requirements proposed in [2], in particular, that a TLS handshake should take place at least every 48 h. Figure 5 shows the maximum number of handshakes for the six selected cipher suites (smallest and largest) and for different SFs. The range is significant. First, there is factor two between the smallest and largest cipher suite which can be observed for all SFs. Second, and even more significant, is the influence of the SF. While for SF 7 almost 7000 handshakes per two days are possible, this value decreases to 147 for SF 12.

Another perspective on the limits of the duty cycle in the downlink is provided in Figure 6. This plot visualizes a variable number of sensors per gateway (from 100 to 50.000) and the minimum time-span between two consecutive TLS handshakes for all sensors connected to that gateway. The plot uses the TLS1.3-S cipher suite. For 50.000 sensors per gateway, a handshake is possible for every SF once a year. For SF 7 and 8 a handshake is possible once a month.

VI. Discussion and Future Work

The combination of LoRaWAN and TLS is an obvious choice to bring end-to-end security to LPWANs. The additional layer of security is often regarded mandatory [2] when LoRaWAN is operated in critical infrastructures like smart

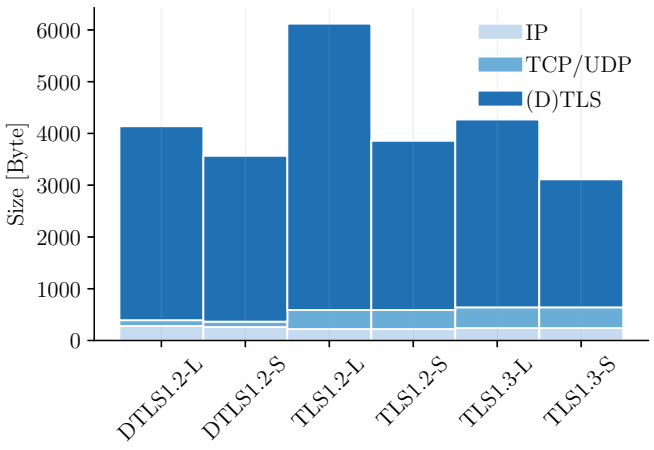

Fig. 3: Cipher suites transmission sizes grouped by layer.

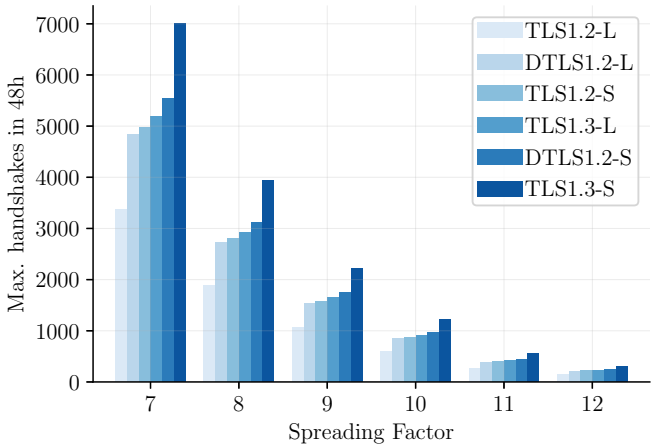

Fig. 5: Maximum number of TLS handshakes in 48 h for different SFs, TLS variants and cipher suites.

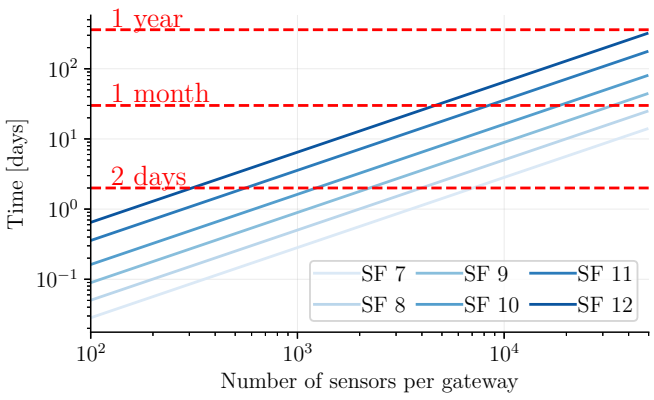

Fig. 6: Minimum time-span between two consecutive handshakes using TLS1.3-S.

energy grids. While LoRa is beneficial for range and energy consumption, the throughput is limited. The operation in a license-exempt band imposes duty cycle restrictions. A mandatory part of TLS is the handshake protocol which includes the transmission of certificates to provide authentication. The transmission size of a full TLS handshakes ranges between 3 kB and 6 kB depending on the cipher suite used.

We have explored the upper bounds for LoRaWAN and TLS by using a verified airtime model. While in the uplink a TLS handshake is regularly possible (i.e. multiple times a day), the duty cycle in the downlink limits the number of senors which can be secured with TLS per gateway. In particular, higher SFs will quickly lead to a bottleneck where only a few hundred sensors can be served per gateway when a full TLS handshake is mandatory after a certain time-span (i.e. every two days). We like to emphasize, that the upper bounds defined in this work are defined due to handshakes only, there is no additional transfer of data included. While this work reveals that for the handshake DTLS has no significant advantage compared to TLS, this likely changes when additional data transmissions are considered.

Selecting a beneficial TLS variant and cipher suite can have an impact of factor two. Notably, for higher SF the completion of a handshake can take more than one hour, if this leads to any timeouts in the protocol needs to be further investigated.

The numbers presented in this work define a best-case scenario where the only sensor data is tramsitted during the handshake. The results are useful to generally assess if TLS and LoRaWAN should be considered for a specific scenario. Possible future work should be directed towards reducing the assumptions we made in this work. In particular, we expect that when realistic packet loss is considered (due to collisions or interference) the number of possible handshakes will be drastically reduced. Incorporating such realistic packet loss into a mathematical airtime model is a challenging task. Retransmission and the state-machine of TLS needs to be modeled accurately. Therefore, future work may consider using an event-drive packet simulation instead of mathemtical model. Another important addition is to use a realistic distribution function for the SFs around a gateway. Such a distribution function can be extracted from the work we provided in [3].

References

[1] M. Centenaro *et al.*, "Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios," *IEEE Wirel. Commun.*, vol. 23, no. 5, oct 2016.

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

[3] M. Rademacher *et al.*, "Path loss in urban lora networks: A large-scale measurement study," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, 2021, pp. 1–6.

[4] H. Linka *et al.*, "Path loss models for low-power wide-area networks : Experimental results using lora," in *VDE ITG-Fachbericht Mobilkommunikation*, 2018.

[5] M. Rademacher, "Code for this work," https://github.com/mclab-hbrs/lora-tls.

[6] M. Saelens *et al.*, "Impact of eu duty cycle and transmission power limitations for sub-ghz lpwan srds: An overview and future challenges," *EURASIP J. Wirel. Commun. Netw.*, vol. 2019, no. 1, p. 1–32, dec 2019. [Online]. Available: https://doi.org/10.1186/s13638-019-1502-5

[7] S. Corporation, "An1200.22 - lora modulation basics," Tech. Rep., 2015.

[8] H. Mroue *et al.*, "Analytical and simulation study for lora modulation," in *25th Int. Conf. on Telecommunications*, June 2018.

[9] L. Alliance, "Lorawan 1.0.3 specification," Tech. Rep., 2017.

[10] C. Pham *et al.*, "Radio channel access challenges in lora low-power wide-area networks," in *LPWAN Technologies for IoT and M2M Applications*. Elsevier, 2020, pp. 65–102.

[11] S.-Y. Wang and C.-H. Chang, "Supporting tcp-based remote managements of lora/lorawan devices," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, 2019, pp. 1–5.

[12] S. Naoui *et al.*, "Enhancing the security of the iot lorawan architecture," in *2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, Nov 2016.

[13] M. Eldefrawy *et al.*, "Formal security analysis of lorawan," *Computer Networks*, vol. 148, 2019.

[14] T. Dierks and E. Rescorla, "The transport layer security (tls) protocol version 1.2," Internet Requests for Comments, RFC Editor, RFC 5246, August 2008.

[15] E. Rescorla, "The transport layer security (tls) protocol version 1.3," Internet Requests for Comments, RFC Editor, RFC 8446, August 2018.

[16] C. Meyer and J. Schwenk, "Lessons learned from previous ssl/tls attacks-a brief chronology of attacks and weaknesses." *IACR Cryptology ePrint Archive*, vol. 2013, 2013.

[17] E. Rescorla and N. Modadugu, "Datagram transport layer security," Internet Requests for Comments, RFC Editor, RFC 4347, April 2006.

[18] P. Weber *et al.*, "Ipv6 over lorawan™," in *2016 3rd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, 2016, pp. 75–79.

[19] I. Butun *et al.*, "Security risk analysis of lorawan and future directions," *Future Internet*, vol. 11, no. 1, 2019.

[20] X. Yang *et al.*, "Security vulnerabilities in lorawan," in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 2018.

[21] F. Hessel *et al.*, "ChirpOTLE: A Framework for Practical LoRaWAN Security Evaluation," may 2020.

[22] I. You *et al.*, "An enhanced lorawan security protocol for privacy preservation in iot with a case study on a smart factory-enabled parking system," *Sensors*, vol. 18, 06 2018.

[23] R. Sanchez-Iborra *et al.*, "Enhancing lorawan security through a lightweight and authenticated key management approach," *Sensors*, vol. 18, 06 2018.

[24] G. Selander *et al.*, "Ephemeral diffie-hellman over cose (edhoc)," Working Draft, IETF Secretariat, Internet-Draft draft-ietf-lake-edhoc-00, July 2020.

[25] C. Zenger *et al.*, "Method for establishing a secure end-to-end connection via lora (wan) tm," Aug 2018.

[26] tanupoo, "Lora time on air calculator," https://github.com/tanupoo/lorawan_toa, (Accessed on 04/11/2022).

[27] D. J. Bernstein *et al.*, "High-speed high-security signatures," *Journal of cryptographic engineering*, vol. 2, no. 2, pp. 77–89, 2012.