Simulative Performance Study of Slotted Aloha for LoRaWAN Channel Access

Frank Loh, Noah Mehling, Stefan Geißler, Tobias Hoßfeld
University of Würzburg, Institute of Computer Science, Würzburg, Germany
{firstname.lastname}@informatik.uni-wuerzburg.de

***Abstract*—Future Internet of Things deployments generate a multitude of new challenges and opportunities. While 5G networks promise massive throughput rates with ultra low delays, many verticals in the areas of Industry 4.0, Smart City, or Smart Agriculture only transmit tiny amounts of data and instead demand high energy efficiency. This is addressed by access technologies like Low Power Wide Area Networks being complementary to high performance 5G networks. Especially Long Range Wide Area Network (LoRaWAN) promises transmissions across long distances with low energy requirements with the drawback of unreliable transmission due to potential message collisions through random channel access. For that reason, a broad parameter study simulation for LoRaWAN channel access with slotted Aloha is presented for real world scenarios and influences like clock drifts or cross traffic. The key impact factors of this channel access approach are studied with focus on the collision probability in various scenarios and simulation results are compared to the current state of the art. The contribution of this work are guidelines for parameter settings in a LoRaWAN with slotted Aloha channel access and performance comparisons for different settings. This information is crucial to scale and operate future LoRaWANs.**

***Index Terms*—Simulation, collision probability, LoRa, IoT**

I. Introduction

Autonomous monitoring and data gathering is one of the most revolutionary, fastest growing, and challenging tasks in this decade. Once an appropriate monitoring system is established in usage areas like Industry 4.0, Smart City, Smart Home, or Smart Agriculture deployments, it yields many benefits. Retrenchment of costs and staff or more accurate information about critical systems are only two possible improvements. Due to the wide range of verticals this technology can be beneficial for, the number and size of deployed of so called Internet of Things (IoT) networks will likely increase manyfold over the next years [1]. To enable this wide variety of use cases to co-exist both logically and geographically, the selection of the correct access technology is essential.

In recent years Low Power Wide Area Networks (LPWANs) have rapidly become established for many application areas [2] because of their simple and cost-efficient deployment. One of the most prominent representatives is Long Range Wide Area Network (LoRaWAN) [3], favorable because of the long transmission range at very low cost. However, LoRaWAN messages are currently transmitted using random channel access because of the simple usage options for all devices. There is no additional need for synchronization or many management traffic. The drawback of this access scheme are quality impairments by message collision and potential data loss. For that reason, lightweight network monitoring approaches as well as general network optimizations are required to ensure reliable and effective operation under various external circumstances and configurations.

One approach to improve transmission quality in LoRaWAN through the reduction of collision probabilities is the adoption of slotted Aloha as channel access scheme [4]. However, this increases the management overhead in the network to keep devices transmitting in predefined slots because of the limiting clock synchronization possibilities in LoRaWAN.

In this work, we present a broad parameter study designed to investigate the impact of various configurations as well as external parameters on the collision probability in LoRaWAN using the slotted Aloha channel access mechanism. Although queueing models revealed the efficiency of slotted Aloha, e.g. [5], a detailed quantification taking into accounts the details of LoRaWan is missing in the literature. We present simulation results highlighting the impact of each key parameter on the transmission quality and highlight generalizable trends inferred from the observations made in this work.

The contributions made in this work are two-fold. First, we present detailed simulation results highlighting the impact of configuration parameters such as the slot length and guard times under different network conditions such as time drifts or cross traffic. Second, we compare the performance of slotted Aloha against the current state of the art using pure Aloha and highlight system performance in real world scenarios. Finally, we make the data obtained in the context of this work as well as simulation code publicly available on GitHub [1] in order to ensure reproducibility.

The remainder of this work is structured as follows. Section II presents background information on LoRa. In Section III related work is presented, followed by the methodology, the scenario overview, and the simulation concept in Section IV. In Section V the presented scenarios are evaluated. Finally, Section VI concludes this work.

II. LoRaWAN Message Transmission

It is crucial to know the characteristics and limitations of the LoRaWAN protocol to understand the implications of the various parameters evaluated later in this work. To this end,

978-1-6654-0601-7/22/$31.00 © 2022 IEEE

[1] https://github.com/lsinfo3/lora_slottedAloha

the following section outlines the main aspects relevant for the remainder of this work. Further transmission specific details are given in e.g. [6] or [7].

The transmission process in state of the art LoRaWAN is very simple and occurs as follows. As soon as a sensor has data to transmit, it selects a transmission channel and sends its data using random channel access without taking other sensors or transmissions into account. For that reason, the main parameters that influence the transmission are the different frequency bands the data can be transmitted on, the available bandwidth (BW), the spreading factor (SF), and the message time on air (ToA) for each transmitted message. In this work, the 868 MHz frequency band (EU868) is used exemplary with 125 kHz channel width, as typically used in Europe. In the following, details about the SF and the ToA as the two main influencing factors of the LoRaWAN protocol are given.

1) Spreading Factor (SF): The LoRa modulation technique used by LoRaWAN is based on the chirp spread spectrum (CSS) technology. Therefore, it uses spread-spectrum modulation to encode symbols that are then transmitted over the air. The SF controls the rate at which chirps occur in this context and hence the speed of data transmission. Every increment of the SF from SF 7 to SF 12 reduces the chirp rate, and thus the transmission rate, by half.

2) Time on Air (ToA): The ToA describes the duration for which a channel is occupied by a transmitting device based on the configured SF and the length of a message in symbols. In the following, both the duration for a single symbol and the total time on air are introduced.

Symbol Duration: The single symbol duration T_s (in seconds) is calculated according to

$$T_\mathrm{s} = \frac{2^{SF}}{BW} = R_\mathrm{s}^{-1}. \tag{1}$$

The number of raw bits a symbol carries is determined by the SF in LoRa. Thus, for a SF of 7, for example, one symbol maps to 7 bit, while one symbol can have more values for larger SFs. Since the symbol duration describes the ToA of one symbol under a specific SF, a higher SF leads to a longer channel occupancy for a single symbol. Furthermore, signals transmitted with larger SFs are more robust against interference and can be transmitted over longer distances or recovered more easily in case of collisions.

LoRa Message: A general LoRa message consists of a preamble, 4.25 symbols for synchronization, an optional header, data payload, and an optional payload CRC field. The possible preamble length n_preamble is between 6 and 65535 symbols, while it is typically 8 symbols for the EU868 band. The number of symbols for the header and payload can be determined as follows.

$$n_\mathrm{payload} = 8 + max(\lceil (n_\mathrm{packet}) \rceil \cdot (CR + 4), 0) \tag{2}$$

with

$$n_{packet} = \frac{(8PL - 4SF + 28 + 16CRC - 20IH)}{4(SF - 2DE)} \tag{3}$$

and the following dependencies.

- Coding rate (CR): 1-4 for different redundancies
- Number of payload bytes (PL) in the range of 1 to 255
- Spreading factor SF in the range of 7 to 12
- Payload redundancy check (CRC) enabled or disabled
- IH as enabled or disabled header
- Low data rate optimization (DE) enabled or disabled

Thus, the total number of symbols for a LoRa message is

$$n_\mathrm{message} = n_\mathrm{preamble} + 4.25 + n_\mathrm{payload}. \tag{4}$$

III. Related Work

LoRaWAN became one of the most promising IoT access technology in recent years. However, due to the random channel access nature, it suffers from message collision and loss. Early studies about the limitations of LoRaWAN are given by [8], [6], with the latter focusing on channel access specifically. Since this work applies a simulative approach to study LoRaWAN channel access, in particular with slotted Aloha to analyze the collision probability, related literature in these research areas is outlined in the following.

Da Silva et al. summarize LoRaWAN simulator tools in a recent survey [9]. The authors list different ns-2, ns-3 as well as OMNeT++ based simulators. Another simulator for LoRaWAN is published recently by Marini et al. [10] called LoRaWANSim. Channel access simulations have been conducted in the past due to the random channel access behavior in LoRaWAN, and thus the occurrence of collision and loss. In a previous work, we have studied the random channel access behavior in more detail to improve successful information transmission [11]. Other approaches study alternative channel access methodologies, like CSMA [12], [13] or a time scheduled approach [14]. Listen before talk is studied in [15] with focus on the coexistence with random access and different channel access approaches are investigated and summarized in [16].

When it comes to the scalability of LoRaWAN networks, Farhad et al. [17] evaluate the performance in urban environments. In a previous study, we focused on scalability and collision probability [18] while the open source tool LoRaPlan [19] presents a software to evaluate custom networks with regard to coverage and collision probability.

Finally, slotted Aloha in the context of LoRaWAN has been studied by different researchers in the past. Polonelli et al. presented an overlay approach for synchronization [20], [4]. Their work show the general usability of slotted ALOHA for LoRaWAN while we extend this idea by an in-depth parameter study and a simulation of a larger number of devices. In addition, other works focus on energy efficiency [21], overhead with regard to throughput and delay [22], or collision avoidance in general [23].

However, to the best of our knowledge, a broad parameter study regarding different parameters for slotted Aloha deployment in LoRaWAN is lacking from literature so far. For that reason, the slot length and guard time for slotted Aloha as well as different SFs and payload sizes for LoRaWAN channel access and occupancy are investigated. Different device clock

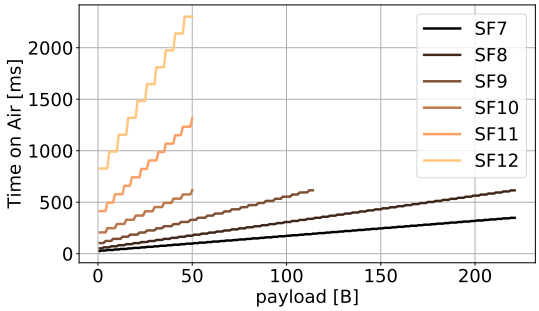


Figure 1: Time on air for different payload sizes.

drifts and cross traffic percentages are considered to emulate more realistic behavior. We developed a lightweight simulation tool for that purpose without the overhead in most well known simulation tools from the literature.

IV. Methodology

The methodology applied during the simulation of the slotted Aloha access mechanism is presented in this section. Important parameters are introduced first, followed by the studied scenarios and the suggested simulation approach.

A. Simulation Parameter Overview

It is necessary to evaluate all SFs when studying the configuration of slotted Aloha parameters to obtain generalizable results due to the interaction between payload length and SF. In LoRaWAN, SF 7 and SF 8 allow 222 B for transmission, for SF 9 it is 115 B and for SF 10, SF 11 and SF 12 it is 51 B in Europe without FOpt [24] for 125 kHz.

With the number of required symbols to transmit one LoRa message described in Equation 4 and the symbol duration from Equation 1, all possible ToA values for specific payload options and SFs can be calculated, visualized in Figure 1. The x-axis shows the payload bytes. On the y-axis the matching ToA value is presented. Each SF is represented in a different color. Note that the same ToA can be achieved by multiple combinations of payload size and SF.

1) Slot Length: The first slotted Aloha related parameter is the slot length. It describes the time between the start of two transmissions. It directly dictates the maximum ToA before causing an overlap with the next transmission slot. However, transmissions with shorter ToAs waste channel resources but can compensate minor inaccuracies in transmission start times for the nodes. However, to avoid complex scheduling overhead for devices and gateways, only uniform slot lengths are evaluated in this work.

2) Guard Time: Guard times represent the time between the end of one slot and the beginning of the next one. Dependent on the timing uncertainty of the synchronization methodology and the inaccuracy of transmission start times of end devices, sensible values must be chosen. The measurements conducted in [4] are used as an estimate for the synchronization error since the synchronization methodology in this work is similar. Thus, it is set to an average of 5.37 ms [4]. The transmission start inaccuracy must also be included in the guard time consideration as it influence the size considerably. The guard time can be expressed as a ratio between the guard time T_g and the slot length T_s. The proposed $T_\mathrm{g}/T_\mathrm{s}$ ratio in [4] is 25 %. However, this work evaluates guard times of up to 30 %.

3) Time Drift: Transmission start inaccuracies are mainly a result of inaccurate clock timings of sensors. They occur due to the nature of oscillator crystals used in low cost devices. These oscillators produce an uncertainty of timing due to running too slow or too fast. This uncertainty can be expressed as a deviation from the nominal frequency in parts per million (ppm). Three common deviations are 20 ppm, creating a timing uncertainty of 200 ms every 2.64 h, 60 ppm, with a timing uncertainty of 200 ms every 53 min, and 80 ppm, creating a timing uncertainty of 200 ms every 40 min, each following a linear behavior [4]. To prevent these time drifts from becoming unmanageable, periodic synchronization is required. If the tolerances for the crystals used in end devices is known, a maximum for the expected time drift can be derived from the clock synchronization frequency. This value can then be used to estimate the appropriate guard time. In this work, all clocks are assumed to run slower than the nominal rate because all clocks cause negative drift. This is a realistic assumption for similar climatic conditions [25].

B. Scenario Definition

To test the slotted Aloha channel access methodology, several scenarios have been defined to determine optimal parameter settings. An overview of all scenarios is given in Table I. In addition to the parameters presented in Table I, the following parameters have been kept constant during all scenarios. The preamble is set to 8 symbols, a CR and CRC of 1 is used with an enabled header and $DE = 1$ for $SF > 10$.

*1) **Scenario S 1:** Optimal Slot Length:* The slot lengths are evaluated using an equivalent payload system for all SFs. Therefore, all slot lengths are defined as duration it requires to transmit a specific number of bytes. Thus, the results are not influenced by the SF and transmissions with different SF are comparable. Different slot length between 1 B and 200 B are studied listed as scenario S 1 in Table I. The studied message payload sizes include 1 B, 4 B, 8 B, 16 B, 32 B with SFs in the range of SF 7 to SF 12 representing a wide range of possible ToA values.

The guard time is set to 0 ms to isolate the impact of slot lengths. Note that this evaluation also studies shorter slot lengths than the ToA to detect possible effects with messages exceeding the maximum slot duration. Re-synchronization of sensors occurs once the time drift exceeds 200 ms. The clock drift behavior of sensors is randomly assigned and uses the following probabilities: 50 % of all transmissions utilize a crystal with 80 ppm drift, 40 % of all transmissions use crystals with 60 ppm drift and 10% of all transmissions use the best 20 ppm crystal (50/40/10 in Table I). A synchronization error of 5.4 ms is considered, matching the average performance of the time synchronization approach proposed in [4].

Table I: Scenario definition overview.

name	study	SF	payload	slot length	guard time	time drifts	cross traffic
S 1	slot length	7-12	1 B, 4 B, 8 B, 16 B, 32 B	1 B, 2 B, 4 B, 8 B, 16 B, 20 B, 32 B, 50 B, 100 B, 200 B	0 ms	50/40/10	0 %
S 2	guard time	7-12	8 B	8 B	1%, 2%, 5%, 7%, 9%, 10%, 12%, 15%, 17%, 20%, 25%, 30%	50/40/10	0 %
S 3	time drift	7-12	8 B	8 B	0 ms	34 ms - 74 ms	0 %
S 4	cross traffic	7-12	8 B	8 B	0 %	50/40/10	0 %, 1 %, 2 %, 3 %, 5 %, 6 %, 7 %, 8 %, 10 %, 15 %, 20 %, 25 %, 30 %, 40 %, 50 %

Table II: Real world scenario definition overview.

name	SF	payload	slot length	guard time	time drifts
S 5.1	7	10 B	10 B	10 %	50/40/10
S 5.2	10	1 B	1 B	10 %	50/40/10
S 5.3	10	51 B	51 B	10 %	50/40/10
S 5.4	12	10 B	10 B	10 %	50/40/10
S 5.5	12	51 B	51 B	10 %	50/40/10

The defined scenario includes a large set of slot length smaller than the ToA, slightly longer, and much longer than the ToA. The goal of this study is to detect thresholds where the overall performance is decreased by too small slot lengths or due to wasted channel resources.

2) ***Scenario S 2:*** *Guard Time Analysis:* In contrast to the slot length study, only a payload of 8 B is chosen as a reference point in the guard time study. To follow the slot length definition laid out, the slot length is fixed to the ToA of the message. The guard times are defined as a percentage relative to the payload size between 1 % and 30 %. Small guard times could be more ineffective for higher SFs and considerably longer ToA values, since more time is wasted due to collisions instead of longer guard times. Relative percentages allow the guard times to be defined consistently between the SFs.

Note that, since device clock drift is the reason for the existence of guard times, no generalizable optimal guard time can be determined from these results. The optimal value depends on the specific network and time drifts. Thus, the evaluation focuses on identifying trends between different guard times, to predict the network performance with different time drift characteristics.

3) ***Scenario S 3:*** *Time Drift Analysis:* Analysis of the time drift behavior is more complex than slot length and guard time studies. Many parameters are kept the same as in the previous investigations. A guard time ratio of 0 % is chosen to also allow a study of small variations in time drift, which could be masked by a guard time otherwise. To study different time drift settings in the LoRaWAN, the three oscillator time drifts established in Section IV-A3 are assigned to different transmissions. The goal is to find overall better or worse time drift behavior, while avoiding a self synchronization between the end device nodes.

In total 10 different combinations of the time drifts are simulated with an average time drift between 34 ms and 74 ms. With these settings it is possible to evaluate small, medium, and large average drifts. Furthermore, device clocks are only re-synchronized when the drift offset is larger than 500 ms compared to 200 ms in the previous studies. With this setting, it is possible to see the influence of different time drifts in more detail without fast re-synchronization. The goal here is to study general trends how time drifts affect the slotted Aloha collision probability.

4) ***Scenario S 4:*** *Cross Traffic:* Since LoRaWAN operates on unlicensed frequency bands, a system running with slotted Aloha can experience interference through other devices utilizing random channel access. One example for such cross traffic is the existence of another separate LoRaWAN in the coverage area.

To test the impact of cross traffic, specific percentages of devices using the pure Aloha channel access methodology are simulated, stated as relative amount of cross traffic in Table I. All other devices utilize slotted Aloha. Which devices utilize pure Aloha is decided randomly before the beginning of the simulation to maintain a uniform distribution of startup times for the devices. All other parameters are kept according to the previous studies and are shown in Table I.

5) ***Scenario S 5:*** *Real World Scenarios:* Finally, after identifying the impact of single parameters, the real world performance of the slotted Aloha channel access methodology is investigated through specific scenarios summarized in Table II. To demonstrate the real world performance, a variety of potential sensor nodes with different transmission characteristics and thus, different ToA values are presented in the following.

Small Periodic Sensor Nodes: LoRaWAN devices typically transmit very short messages and with a low SF [26]. This real world scenario will be replicated by evaluating nodes transmitting 10 B payloads using SF 7 (S 5.1). This leads to a ToA of 41.2 ms. However, a higher SF is required if these devices are located further away from the gateway. This is emulated by the same sensor nodes on transmitting with SF 12 and thus, a ToA of 1155 ms (S 5.4).

Binary Sensors: In contrast to the previous example, many LoRaWAN devices need to transmit a binary status

change only. Examples are parking lot sensors or door sensors which only transmit a status bit every time, the occupancy status changes in case of the parking lot sensor. This scenario requires only a payload pf 1 B and the ToA is only influenced by the required SF. If SF 10 is required for this scenario S 5.2, a ToA of 206.8 ms is achieved.

Weather Station: A near maximum payload is, for example, transmitted by weather stations using the message format laid out in [27]. The individual messages are 11 B in size. However, data are often aggregating to save overhead. This can lead to the maximum number of transmittable bytes. This is simulated with 51 B payload in scenario S 5.3 and scenario S 5.5 respectively. If devices are located far enough from the gateway to need SF 10 for transmission, a ToA of 616 ms is produced. If SF 12 is required for devices with large distance to the gateway, this example weather station can reach the maximum possible ToA in a LoRaWAN with 2301.9 ms.

C. Simulation Concept

The simulation conducted in this work models the traffic produced by individual nodes in the network. It is assumed that each node transmits data once a time frame. Note that other transmission models can be simulated by allocating multiple time slots per sensor. The lightweight simulation is written in Python and requires very little overhead in contrast to more detailed simulators based on, for example, OMNeT++ or ns-3. The general approach consists of five steps and is described in detail in the following.

Step 1 - Initialization: The simulation parameters are defined in the first step. For each simulation run, up to 10,000 sensors are simulated in steps of 10 sensors to see the behavior for different network sizes. Further parameters, like simulated sensor clock drift and potential cross traffic percentage are defined in this step as well.

Step 2 - Sensor setup: Next, each node receives an initial random transmission start time within a given time frame. For this implementation a time frame of one hour is selected. Note that other time frames do not change the behavior or the simulation but only the density of simulated transmission attempt. Then, the chosen time frame is split in equal length slots with the predefined slot lengths from Table I. The start timestamp of each slot is a possible transmission start timestamp for the slotted Aloha approach. If the transmission start time is not equal to a slot start timestamp, the sensor is shifted to the following slot starting its transmission at the beginning.

Step 3 - Message creation: In the message creation step, a single message containing the timestamp of the transmission start time, the number of bytes, and the SF is created for each sensor node. With the number of bytes and the SF, the ToA and thus, the transmission end timestamp is calculated and added to the message. Furthermore, the synchronization error and the time drift experienced relative to the nominal timing is allocated to the sensor.

Step 4 - Transmission: In the transmission step, it is checked whether transmission intervals consisting of transmission start and transmission end timestamp overlap. Messages from sensors with overlapping intervals are counted as colliding, other messages as successfully transmitted. Furthermore, sensors with total time drifts of more than 500 ms in scenario S3 and 200 ms for all other scenarios are re-synchronized with a synchronization message of 1 B payload. Note that the re-synchronization is created as an additional message in the network, and thus, other messages can collide with it. However, it is assumed that the re-synchronization message is always transmitted correctly. In reality this can be achieved when transmitting the re-synchronization for all sensors in an independent channel or with higher transmission power and the largest SF in the network. According to [28] messages with stronger signal and higher SF can be received correctly while other colliding messages are lost.

Step 5 - Transmission end: Finally, the time drifts are recalculated for each sensor based on the last synchronization time. Then, the sensors enter a sleep time to the next transmission hour and the next transmission cycle starts with **Step 2** where each sensor transmits periodically in the same time slot only influenced by the clock drift.

In this work, a simulation time of 24 h is used. At the beginning of each simulation, a transient phase is detected before the system enters steady state. For that reason, the first 5 h of each simulation run are not considered in the data evaluation and to provide the steady-state results. Please note that the messages transmitted with the pure Aloha approach in the cross traffic scenario S 4 are randomly generated for each device in each transmission time frame.

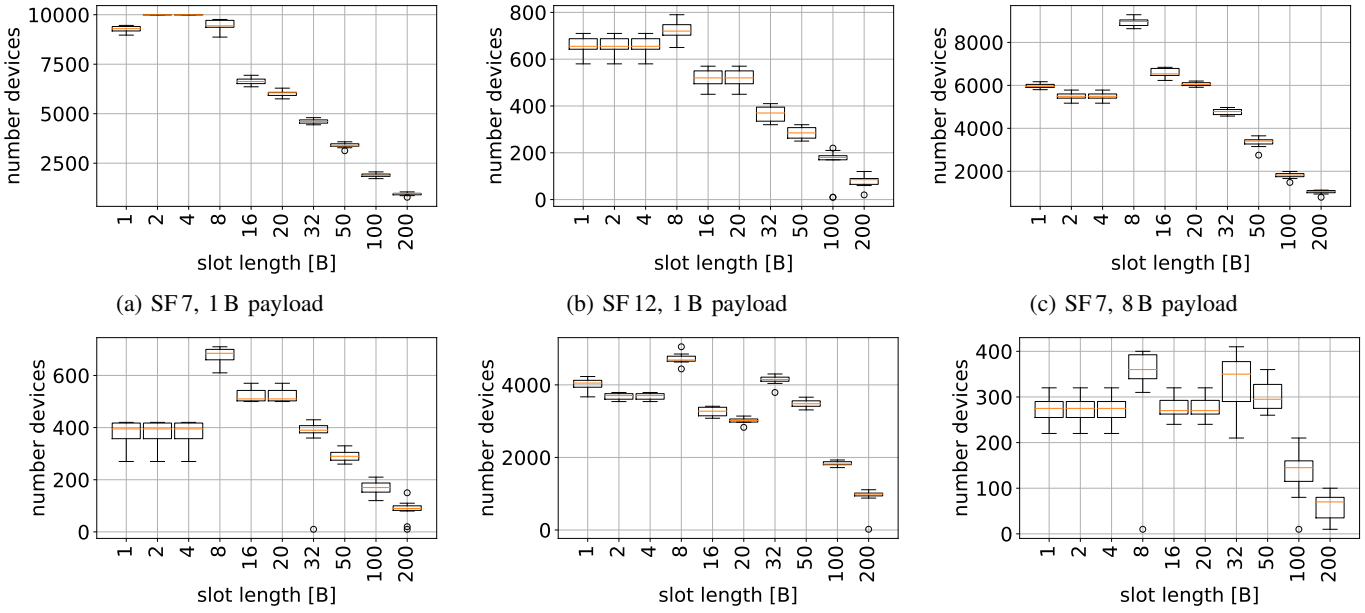
V. Evaluation

The following section presents the results obtained by applying the outlined methodology to the scenarios defined in Table I as well as the real world scenarios of Table II.

A. Optimal Slot Length

Figure 2 presents the results for the slot length study for 1 B, 8 B, and 32 B payload transmitted with SF 7 and SF 12, respectively. Studies of other SFs show similar results with other device limits only. For that reason, only SF 7 and SF 12 is analyzed in detail as minimal and maximal SF value. The x-axis shows the slot length in byte according to the definition in Section IV-B, the y-axis plots the number of devices a network can sustain, before a collision probability of 5 % for SF 7 or 10 % for SF 12 is surpassed. Different thresholds are selected to better highlight the effects of each parameter, as SF 12 surpasses the 5 % threshold already with a very little number of devices.

The individual runs are presented as boxplots where the median of 10 runs is represented by the orange line, with the box representing the 25 % and 75 % quantiles. The whiskers indicate a distance of 1.5 times the interquartile range above and below the upper and lower quartiles. As a result, higher values on the y-axis show better network performance in terms of collision probability. The general findings are similar for



(a) SF 7, 1 B payload (b) SF 12, 1 B payload (c) SF 7, 8 B payload

(d) SF 12, 8 B payload (e) SF 7, 32 B payload (f) SF 12, 32 B payload

Figure 2: Maximum number of devices in a network without exceeding 5 % collision probability (SF 7) or 10 % collision probability (SF 12) for different slot lengths and payload sizes.

other thresholds, as the general trend for each SF remains similar.

The evaluation for a payload of 1 B is shown in Figure 2a and Figure 2b respectively. There, no slot lengths shorter than the ToA could be evaluated as 1 B is the minimal possible payload and thus ToA for each SF. When the messages are transmitted with SF 7, slot lengths slightly larger than the ToA perform best. The 5 % collision probability threshold is not reached for 10,000 devices for a slot length of 2 B or 4 B. Thus, both slot length values show the best results followed by 8 B and 1 B. A longer slot length equivalent to 8 B payload performs best for SF 12 presented in Figure 2b. The slot length of 1 B matching the ToA performs similar to 2 B and 4 B. However, slot lengths longer than 8 B show worse results. Thus, longer slot lengths of especially 8 B show the best result for SF 7 and SF 12 to transmit only 1 B payload, although channel resources are wasted. This demonstrates the importance of guard times especially for very small payload.

When the payload size is increased to 8 B, as shown in Figures 2c and 2d, the behavior changes slightly. Note that since the result for 4 B, 8 B and 16 B payload behave similar, only 8 B is presented in the following. For SF 7, the payload of 8 B results in a ToA of 36 ms, which matches the peak in the maximum number of devices in Figure 2c. For SF 12 plotted in Figure 2d, the largest number of devices is also achieved with a slot length of 8 B. This is equal to 991 ms for SF 12 and matches the ToA of the message. Thus, for both SFs the best slot length is equal to the ToA of the message while slightly larger values outperform slightly smaller values a little. This effect is larger for larger SFs.

A different result is visible for larger payloads. Figure 2e shows the results for 32 B payload transmitted with SF 7. There, one anomaly is detected. The slot length matching the payload of 8 B performs best, even though it is considerably shorter than the ToA of the message. This is most likely a result of the ratio between the ToAs. 8 B slot length results in 41 ms ToA. The ToA to transmit 32 B is 77 s and thus, nearly double the ToA required to transmit 8 B. This allows two slots to cover a single transmission without much overlap. The same behavior is visible for SF 12 shown in Figure 2f. However, no clear difference is visible here for slot lengths between 1 B and 50 B.

In general, the study shows that slot lengths matching the ToA of the transmission performs good for all demonstrated SFs, as well as all other evaluated SFs. For small payloads, slots lengths slightly larger than the transmission ToA perform best, especially for small SFs while for all payloads it is visible that too large slot length perform worst. If the slots are too large, many channel resources are wasted and it is not possible for all devices to find an empty or available slot.

Thus, in general it is advisable to use a slot length matching the ToA of the transmission while for small payloads and SFs, guard times are especially important.

B. Guard Time Analysis

In the guard time study, the influence of different guard time duration on the network performance is studied. Figure 3 shows the number of devices, before the network experienced 5 % collision probability on the y-axis. The x-axis shows the guard time between the slots as a percentage. This percentage is multiplied with the slot length to calculate the actual guard time. The colored boxplots represent the results of the

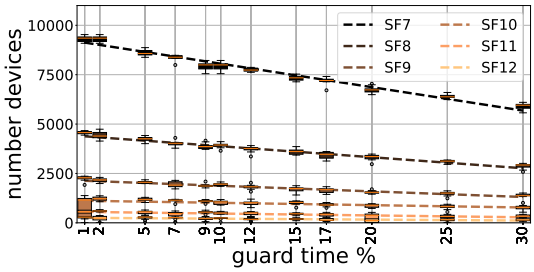


Figure 3: Guard times with linear fit.

simulation, while the dashed lines of the same color represent a linear fit.

All SFs follow a linear decline in the number of supported devices and therefore, a higher collision probability. Especially for small SFs, the slope of the linear fit is larger. For that reason, small guard time increases influence the overall performance more. This allows larger SF values to utilize much longer guard times without large impact on the device capacity. As a result, utilizing a higher SF for devices with worse clock accuracy is recommended, since longer guard times are possible before a negative impact on the network is achieved. This, however, has to be balanced with the inherently lower overall device capacity for larger SFs. Furthermore, as shown in the slot length study, the guard time is especially important for small SFs. Since other tested collision probability values show similar results, they are not plotted.

The summary of this study shows that guard times are especially important for small SFs and small payloads. The length of the guard time should be adjusted according to the sensor clock drifts in the network.

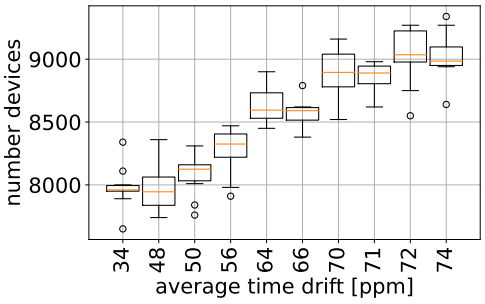
C. Time Drift Analysis

The time drift analysis result shows an unexpected outcome. The number of possible devices increases for lower SFs, if the average time drift increases. This is shown in Figure 4a for SF 7. The x-axis presents the average time drift of the tested devices and the y-axis plots the number of devices the network could accommodate before a collision probability of 5 % is exceeded. Networks with higher average time drift generally perform better, than networks with a lower average time drift at the cost of consistency between the runs for SF 7. One reason for this behavior is the small slot length where a message can skip a complete slot and thus, another potential source for collisions with a large time drift. This is not possible with a large SF and longer slots for the studied time drift range. Thus, the impact of the time drift stabilizes, with SF12 showing no clear affect of different time drifts on the network performance shown by Figure 4b.

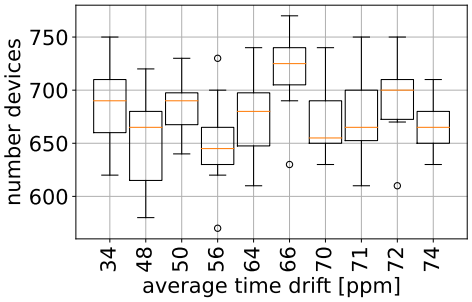
Thus, different average time drifts have more influence in networks with smaller SFs and thus, slot lengths.

D. Cross Traffic Analysis

The cross traffic result shows a comparatively high run to run variance. This is an effect of the random assignment of transmission start times for devices transmitting with pure

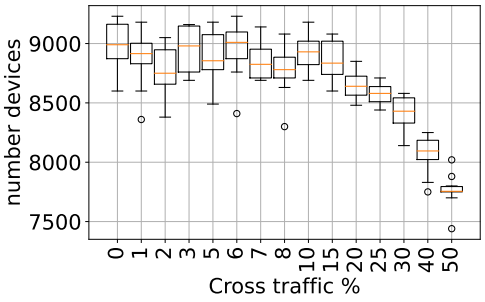


(a) SF 7

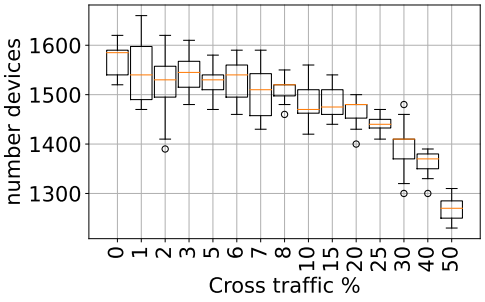


(b) SF 12

Figure 4: Maximum number of devices in a network without exceeding 5 % collision probability (SF 7) or 10 % collision probability (SF 12) for different average time drifts.



(a) SF 7



(b) SF 12

Figure 5: Maximum number of devices in a network without exceeding 10% collision probability for different cross traffic percentages and SFs.

Aloha or slotted Aloha. In the following SF 7 and SF 12 is presented only since the other SFs show similar behavior while the collision probability is increasing with the SF.

Figure 5a shows the results for SF 7. The x-axis shows

Table III: Slotted Aloha to pure Aloha comparison.

name	SF	payload	slot length	guard time	time drifts
pure	7-12	8 B	N/A	N/A	N/A
slotted	7-12	8 B	8 B	10 %	50/40/10

the different cross traffic percentages, the y-axis shows the number of devices a network can accommodate. The network performance does not decrease in this scenario for up to 15 % cross traffic. However, a linear decrease in device capacity can be observed for more cross traffic. In contrast, Figure 5b shows the results for SF 12. The results with little cross traffic show a high variability for this SF, most likely due to the low number of devices achievable in the network. However, a small decrease in the number of devices is visible with increasing cross traffic. This behavior is accelerated starting from 20 % cross traffic and more.

In conclusion, slotted Aloha can tolerate some cross traffic with little to no impact on the collision probability.

E. Comparison to Pure Aloha

This section compares the performance of slotted Aloha to pure Aloha for LoRaWAN, using information for parameter settings obtained from previous simulation results. The important parameters are presented in Table III.

The payload is set to 8 B to preserve integrity with previous tests. The slot length which matches the ToA of the message performed best in the evaluation and is applied for this comparison. The guard time set to 10 %, as the results demonstrated that a small guard time is required, especially for small payloads. The time drift configuration for the network is 50/40/10 as introduced in Section IV-A3 and used for the other scenarios. The pure Aloha results are achieved with an identical configuration for the payload. The slot allocation and the time synchronization is removed in the simulation. This replicates a pure Aloha network with devices following the same transmission pattern as the slotted Aloha network, but without the consideration for time slots and synchronization. The collision probability with pure Aloha is 67 % higher than with slotted Aloha for SF 7. For SF 8 it is still 62.5 % higher and 60.9 % for SF 9. SF10 shows a 55.3 % increase, SF11 a 46.5 % increase, and SF12 an increase of 32.2 %. The results show that slotted Aloha performs better than pure Aloha, however the collision probability advantage of slotted Aloha diminishes with an increasing SF. As a noteworthy result, slotted Aloha allows the devices to utilize SF 12, instead of SF 11 while retaining the same collision probability as pure Aloha for more than 5,000 sensors. In a real deployment however, the network would experience a collision probability of more than 50 %, making it unfeasible.

F. Real World Scenarios

The result for the real world scenario simulation defined in Table II is summarized in Figure 6. The figure shows the collision probability difference when slotted Aloha is used

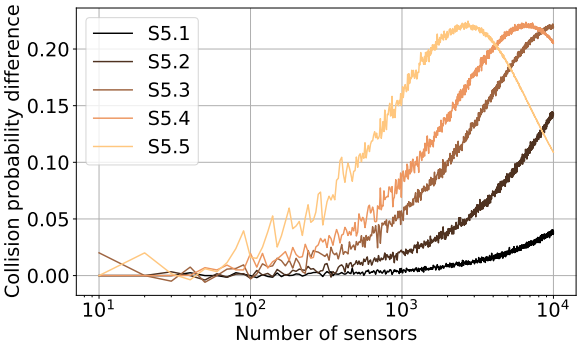


Figure 6: Collision probability difference slotted Aloha and random access for all real world scenarios.

compared to a channel access with pure Aloha on the y-axis. Positive values represent an improvement if slotted Aloha is used. The x-axis shows the simulated number of sensors.

The scenarios with larger scenario numbers use larger SFs for transmission. Thus, the required ToA for transmission is also increasing. The influence of this behavior on the result is visible in the figure. Slotted Aloha performs better compared to pure Aloha for all scenarios. However, when a specific number of sensors in the network is reached, the improvement peak is reached and the benefit from using slotted is declining again. In these cases, the network is already in an overload situation where, e.g., all slots are already in use. This improvement peak is reached with larger ToAs for fewer sensors. The maximal possible improvement for using slotted Aloha is 22.4 %. This value is similar for all scenarios.

Thus, up to a specific number of sensors, slotted Aloha always outperforms state-of-the-art random channel access in real world scenarios dependent on the transmission ToA.

VI. Summary

LoRaWAN is one of the most interesting but also challenging access network technologies for future IoT. With the currently used random channel access approach, the potential for message collision and data loss is considerably high. Thus, the full potential of this technology is not used so far.

In this work, we study slotted Aloha as an alternative to the random channel access approach with a comprehensive parameter study. The results show the benefits of using slotted Aloha channel access with improvement rates of 22 % up to 67 % dependent on the scenario and LoRa message parameters.

Furthermore, it is shown that appropriate parameter settings for the slotted Aloha approach can increase the number of supported sensors massively. The most important parameters are exposed to be the slot length and the guard time setting, especially to transmit small messages with small SFs. In addition, it is shown that slotted Aloha can also coexist with up to 15 % cross-traffic without significant collision probability increase.

References

[1] Statista, "Internet of Things (IoT) and non-IoT Active Device Connections Worldwide from 2010 to 2025," 2021. [Online]. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

[2] I. Now, "Cellular MNOs are Increasingly Offering Access to more than one LPWAN Technology," 2018. [Online]. Available: https://www.iot-now.com/2018/10/29/89895-lpwan-fastest-growing-iot-communication-technology/

[3] I. Analytics, "LPWAN Emerging as Fastest Growing IoT Communication Technology," 2018. [Online]. Available: https://iot-analytics.com/lpwan-market-report-2018-2023-new-report/

[4] T. Polonelli, D. Brunelli, A. Marzocchi, and L. Benini, "Slotted ALOHA on LoRaWAN - Design, Analysis, and Deployment," *Sensors*, 2019.

[5] P. Tran-Gia and T. Hoßfeld, *Performance Modeling and Analysis of Communication Networks*. Würzburg University Press, 2021. [Online]. Available: https://modeling.systems

[6] D. Bankov, E. Khorov, and A. Lyakhov, "On the Limits of LoRaWAN Channel Access," in *International Conference on Engineering and Telecommunication (EnT)*. IEEE, 2016.

[7] C. Goursaud and J.-M. Gorce, "Dedicated networks for IoT: PHY / MAC State of the Art and Challenges," *EAI endorsed transactions on Internet of Things*, 2015.

[8] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *Communications magazine*, 2017.

[9] J. C. da Silva, D. d. L. Flor, V. A. de Sousa Junior, N. S. Bezerra, and A. A. de Medeiros, "A Survey of LoRaWAN Simulation Tools in ns-3," *Journal of Communication and Information Systems*, 2021.

[10] R. Marini, K. Mikhaylov, G. Pasolini, and C. Buratti, "LoRaWANSim: A Flexible Simulator for LoRaWAN Networks," *Sensors*, 2021.

[11] F. Loh, S. Raffeck, F. Metzger, and T. Hoßfeld, "Improving LoRaWAN's Successful Information Transmission Rate with Redundancy," in *17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMoB)*. IEEE, 2021.

[12] N. Kouvelas, V. Rao, and R. Prasad, "Employing p-CSMA on a LoRa Network Simulator," *arXiv preprint arXiv:1805.12263*, 2018.

[13] T.-H. To and A. Duda, "Simulation of LoRa in ns-3: Improving LoRa Performance with CSMA," in *International Conference on Communications (ICC)*. IEEE, 2018.

[14] F. Loh, N. Mehling, and T. Hoßfeld, "Towards lorawan without data loss: Studying the performance of different channel access approaches," *Sensors*, 2022.

[15] J. Ortín, M. Cesana, and A. Redondi, "How do ALOHA and Listen Before Talk Coexist in LoRaWAN?" in *29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2018.

[16] L. Beltramelli, A. Mahmood, P. Österberg, and M. Gidlund, "LoRa Beyond ALOHA: An Investigation of Alternative Random Access Protocols," *Transactions on Industrial Informatics*, 2020.

[17] A. Farhad, D.-H. Kim, and J.-Y. Pyun, "Scalability of LoRaWAN in an Urban Environment: A Simulation Study," in *11th International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2019.

[18] F. Loh, D. Bau, J. Zink, A. Wolff, and T. Hoßfeld, "Robust Gateway Placement for Scalable LoRaWAN," in *13th IFIP Wireless and Mobile Networking Conference (IFIP WMNC)*. IEEE, 2021.

[19] F. Loh, N. Mehling, F. Metzger, D. Hock, and T. Hoßfeld, "LoRaPlan: A Software to Evaluate Gateway Placement in LoRaWAN," in *17th International Conference on Network and Service Management (CNSM)*. IEEE, 2021.

[20] T. Polonelli, D. Brunelli, and L. Benini, "Slotted ALOHA Overlay on LoRaWAN - A Distributed Synchronization Approach," in *16th international conference on embedded and ubiquitous computing (EUC)*. IEEE, 2018.

[21] L. Beltramelli, A. Mahmood, P. Österberg, M. Gidlund, P. Ferrari, and E. Sisinni, "Energy Efficiency of Slotted LoRaWAN Communication with out-of-band Synchronization," *Transactions on Instrumentation and Measurement*, 2021.

[22] I. Cheikh, E. Sabir, R. Aouami, M. Sadik, and S. Roy, "Throughput-Delay Tradeoffs for Slotted-ALOHA-based LoRaWAN Networks," in *International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2021.

[23] L. Xiongfei, Z. Yunyi, and B. Liao, "LoRaWAN Anti-Collision Algorithm Based on Dynamic Frame-Slotted ALOHA," in *Journal of Physics: Conference Series*. IOP Publishing, 2020.

[24] "LoRaWAN Regional Parameters v1.1rA," accessed: 2021-10-27. [Online]. Available: https://lora-alliance.org/resource_hub/lorawan-regional-parameters-v1-1ra/

[25] T. Schmid, Z. Charbiwala, J. Friedman, Y. H. Cho, and M. B. Srivastava, "Exploiting Manufacturing Variations for Compensating Environment-Induced Clock Drift in Time Synchronization," *ACM SIGMETRICS Performance Evaluation Review*, 2008.

[26] N. Blenn and F. Kuipers, "LoRaWAN in the Wild: Measurements from The Things Network," *ArXiv*, 2017.

[27] "MeteoHelix Open Message Format," accessed: 2021-10-27. [Online]. Available: https://www.baranidesign.com/meteohelix-message-decoder

[28] J. Haxhibeqiri, F. Van den Abeele, I. Moerman, and J. Hoebeke, "LoRa Scalability: A Simulation Model Based on Interference Measurements," *Sensors*, 2017.