A New Planning-Based Collision-Prevention Mechanism in Long-Range IoT Networks

Jakub Pullmann and Dominik Macko, *Member, IEEE*

***Abstract*—Wireless communication is prone to collisions, resulting from multiple devices transmitting at the same time. It implies subsequent retransmissions, which increase energy consumption of communicating devices and reduce throughput of the network. This is especially critical in Internet of Things (IoT) networks, in which the number of connected devices grows rapidly and the available energy of IoT end devices is rather limited (e.g. energy harvesting, battery powered). The number of retransmissions must be reduced in order the networks to be sustainable. However, in long-range wireless IoT networks, the most effective collision-resolution techniques using a transmission-channel listening to detect collisions cannot be reliably used due to various problems, such as a hidden-node problem or environment interference. In this article, a new solution of this problem is proposed, which consists of a new communication-planning mechanism for low-speed long-range IoT networks with a huge number of communicating energy-constrained devices. The access points (or IoT gateways) are used to plan the periodically repeated communication into a transmission schedule, allowing only a single IoT device to communicate at a time. This approach results in reduction of collisions, which leads to increased network throughput, smaller delays, and lower power requirements of energy-constrained devices. The experiments indicate that the proposed approach provides better communication efficiency than the LoRaWAN and Sigfox collision-resolution techniques, when more than 15, respectively 125, end devices communicate with a single access point.**

***Index Terms*—Energy efficiency, collision prevention, Internet of Things, long-range networks, low-power communication, wireless sensor networks.**

I. Introduction

THE Internet continues to evolve and one of its newest dimensions is represented by the Internet of Things (IoT) [2]. It is a network of interconnected smart devices that brings new opportunities for aggregating, analysing, and distributing information, which enable to create new knowledge and make more informed actions. IoT devices now influence our everyday lives, being incorporated into our surroundings. They are used in such areas as transportation, agriculture, energetics, trade, healthcare, or education [3]. There are many use cases of IoT in these areas, such as home automation, health monitoring, traffic or parking management [4]. However, new IoT applications in new areas are continuously emerging [5], [6], [7], [8], which implies a rapid growth of IoT. The number of IoT devices in 2018 was estimated to 10 billion, which should increase to 64 billion by 2025 (according to [9]), and to 500 billion by 2030 (according to Cisco [10]). Such predictions puts IoT sustainability in doubt, concerning about a high amount of energy consumed by these devices.

Nevertheless, the low power consumption is one of the most critical aspects in most of the IoT devices. The reason is not only the sustainable growth, but also because the IoT devices are often powered by batteries or some alternative power sources (e.g. energy harvesting [11]). Due to the mobility and flexibility, they just cannot be connected to the electrical grid. This brings multiple disadvantages, such as a lower power output of alternative power sources, a limited capacity of batteries, or a complicated and expensive maintenance. Therefore, the power consumption of IoT devices must be reduced as much as possible.

In IoT networks, various communication technologies can be used to provide a wireless connection, such as LoRaWAN, Sigfox, ZigBee, Z-Wave, Thread, Bluetooth Low Energy, or WiFi-ah. These technologies offer different speed and range, use different frequencies and medium-access techniques, and have different energy requirements. Wireless IoT networks are especially prone to collisions, resulting from simultaneous data transmission of multiple devices. A collision causes a loss of the transmitted data, which affects reliability of delivery or causes retransmissions. Retransmissions directly impact the energy consumption of IoT devices, since they need to process and send more messages. Retransmissions also decrease the network throughput and increase transmission delays [12], [13]. The probability of a collision is affected by various factors, such as the number of devices, the communication speed, the size of transmitted messages, or the time on air parameter [14]. The continuously increasing number of devices in IoT networks makes them especially vulnerable against collisions, which makes the collisions a problem that must be coped with.

Sigfox uses a very simple collision-resolution technique [15]. The transmitting device does not listen to the communication channel prior to the transmission, instead, it transmits the message three times – i.e. in three different time intervals and each time at a random frequency channel. Such an approach is simple to use to increase the probability of successful delivery of the message. Although it is usable

Manuscript received May 17, 2019; revised July 18, 2019.

This is an extended version of the paper accepted at the TSP 2019 conference [1].

This research was partially funded by by the Slovak Research and Development Agency (APVV-15-0789), the Slovak Cultural and Educational Grant Agency (KEGA 011STU-4/2017), the Slovak Scientific Grant Agency (VEGA 1/0836/16), the project "University Science Park of STU Bratislava" (ITMS 26240220084), co-funded by the European Regional Development Fund, and the projects no. 2018/14427:1-26C0 and 002STU-2-1/2018.

J. Pullmann and D. Macko are with the Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava, Ilkovičova 2, 842 16 Bratislava, Slovakia e-mail: xpullmann@stuba.sk, dominik.macko@stuba.sk.

to deal with collisions or environmental interference for the single transmitted message, the redundant messages increase the collision probability for other communications. It could become counter-productive in a case of high number of devices in the network. The redundant transmissions (often unnecessary) increase the energy consumption (approximately three times) and consume more network bandwidth, which represents enormous overhead of the technique.

The LoRaWAN protocol uses a different collision-resolution technique [12]. Although the device also does not listen to the communication medium before the transmission, the message is transmitted only once in case of LoRaWAN. A commonly used acknowledgement message (ACK) is used to identify that the message was successfully delivered. If the transmitting device does not receive the corresponding ACK in the predefined time period (i.e. a collision has occurred), it retransmits the message after an exponential back-off time. This technique ensures the reliable delivery and consumes less bandwidth than the Sigfox technique. However, the acknowledgement message also requires processing (consuming energy) and can be lost during transmission (causing the retransmission although the original message was delivered). Nevertheless, it should perform better than Sigfox in a case of a high number of devices connected to the network. As discussed in [16], the scalability of LoRaWAN solution is limited by the duty-cycle restriction (limiting the time-on-air for IoT end nodes) and data rate (throughput is limited by collisions for low data rates). The recent on-demand TDMA (Time Division Multiple Access) [17], [18] and LPWA-MAC (Low-Power Wide-Area Medium Access Control) [19] approaches help to overcome this LoRAWAN limitation by modifications of its medium access protocol.

The ZigBee technology uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) technique to cope with collisions, which is a collision-prevention technique well-known from the standard WiFi networks [20]. Since ZigBee is focused on short-range communication (unlike LoRaWAN and Sigfox), it can listen to the communication channel to check its availability. If the medium is not occupied, the transmitting device can send the message. When the communication medium is not free, the device waits for an exponential back-off time and listens to the channel again. Since devices cannot transmit and listen simultaneously, they cannot detect the collisions while transmitting. The collision thus can occur, if multiple devices start to listen at the same time. To deal with such a problem, the techniques such as WCSMA/CD (Wireless Carrier Sense Multiple Access with Collision Detection) and CSMA/CR (Carrier Sense Multiple Access with Collision Resolution) have been developed. These techniques use small random time periods to pause the transmission and listen to the channel to identify a collision. The key drawback of this approach is a problematic implementation of the collision-detection slots with optimal length. These techniques are evaluated in [21]. However, the distance and environment interferences affect the reliability of communication-channel listening, which impacts the effectiveness of these techniques. Another approach, called HSW-802.15.4 [22], combines the strengths of CSMA/CA and TDMA. After a collision occurs, the device is put to sleep for a specific time, based on the schedule information broadcasted by the coordinator. The EEMIP approach [23] uses an application layer to schedule the communication into timing channels to avoid collisions and uses the concept of priorities to increase the quality of service in ZigBee networks.

This article deals with long-range low-speed wireless IoT networks connecting via network access points (such as Sigfox or LoRaWAN). A special focus is targeted on various IoT sensor devices that periodically send the measured data (most of the IoT-based heterogeneous wireless sensor networks). In such networks, the highly effective collision-resolution techniques using listening of transmission channel cannot be reliably used due to various problems (e.g. a hidden-node problem or environment interference). We find the used collision-resolution techniques in the analyzed long-range IoT networks as not effective enough for the incoming future IoT growth. Therefore, we have proposed a new more effective collision-prevention technique based on communication-planning mechanism, using which only a single device is communicating in a given time slot and thus collisions are avoided. The key contribution of this article consists of the following:

- *SCPP (Slot-based Communication Planning Protocol) design* – a control protocol for communication scheduling to avoid collisions.
- *Increased scalability* – the proposed collision-prevention technique is more scalable than the existing techniques.
- *Increased network throughput* – a reduced number of redundant messages increases the efficiently utilized bandwidth.
- *Increased energy efficiency* – a reduced number of collisions and retransmissions reduces the amount of wasted energy.
- *Increased quality of service* – an increased efficiency of bandwidth utilization increases the probability of successful delivery of a message on the first attempt.

The article is structured in the following way. In Section II, the proposed communication-planning mechanism, along with the corresponding control protocol, is described. The experimental results are outlined in Section III and discussed in Section IV. Conclusions are given in Section V.

II. The Proposed Planning Mechanism

The proposed method targets the long-range IoT networks, in which the sensor-based end devices communicate periodically (i.e. periodically sends the measured data), and the communication is centralized via network access points (APs). In such networks, the majority of communication is transmitted in uplink direction (i.e. from an IoT sensor end device to the AP). The key feature of these networks is that the communication is predictable – i.e. parameters such as the data size, the periodicity, and the communication time can be predetermined. Suitable application scenarios include those Sigfox and LoRa use cases [24], [25] focused on monitoring rather than event-based alerts (e.g. the parking-space occupancy can be monitored each five minutes, the environment temperature can be

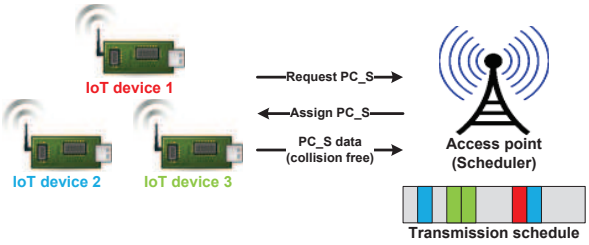

Fig. 1. The basic principle of the proposed communication-planning mechanism.

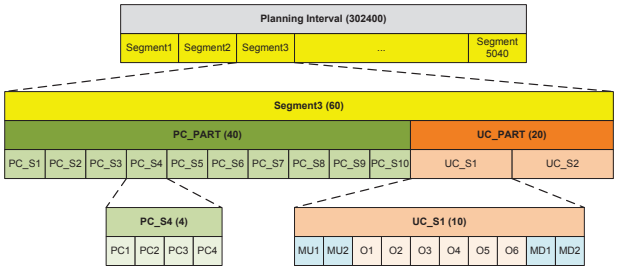

Fig. 2. The transmission-schedule structure.

sensed every hour, and weight of a bee hive is measured only once a day). Such information is used by the proposed method to accordingly plan the communication in order to maximize the efficiency.

The key part of the proposed collision-prevention mechanism is a new communication-planning protocol (Slot-based Communication Planning Protocol – SCPP). This protocol utilizes an exchange of control messages between an end device and the AP to assign a time slot for planned communication to the end device. The next important part of the proposed method is the transmission schedule, which is created and maintained by the AP. It is used to split the continuous time into two types of time slots, for planned and unplanned communication. The time slots for planned communication (PC_S) can be assigned to end devices, which use them for transmission of periodic communication (i.e. periodically measured sensor data). One PC_S can be assigned to a single end device only (i.e. a single device is transmitting at a time), meaning that the collisions are avoided since no simultaneous communication occurs during PC_S. However, a single end device can have multiple time slots assigned, which enable it to send data from various sensors with different periodicity or data size. The time slots for unplanned communication (UC_S) are shared and cannot be assigned to any specific device (i.e. collisions can occur in these slots). The collisions in UC_S are resolved using the slotted ALOHA technique. These slots are reserved for control messages and communication that could not be predetermined (e.g. event-based alerts). Fig. 1 illustrates the basic principle of communication scheduling using the proposed method. The IoT devices 1–3 represent sensor-based end nodes, which need to request PC_S from the AP to communicate. The AP assigns suitable free slots in the transmission schedule based on the request and reports the assigned slots to the end devices. Afterwards, the end devices can send the sensed data during the dedicated time slots without collisions. Since the IoT communication is heterogeneous, the slots are assigned according to specific needs of a given device (more or less frequent), as indicated by the colors in the transmission schedule (corresponding to different IoT devices).

The transmission schedule is created for a time frame of the Planning Interval (e.g. a week or a month) that periodically repeats. The Planning Interval is divided into a specific number of Segments, which have the same structure. Each Segment includes two parts, for planned communication (PC_PART) and for unplanned communication (UC_PART). PC_PART consists of a specific number of time slots (PC_S) that can be assigned to end devices by the AP. A specific number of messages can be sent in each PC_S, meaning that the end device can send for example four data messages in the reserved time slot, not just one. UC_PART also consists of a specific number of time slots (UC_S) that are used for control messages (MU – management uplink, MD – management downlink) and other unplanned communication (O). The length of the Planning Interval as well as the number and size of time slots are not predefined by the SCPP protocol. These parameters must be configured for a specific network (based on characteristics of the expected traffic and the used communication technology) and can be dynamically adjusted by the AP according to the current situation.

To better illustrate the proposed structure of the transmission schedule, an example is provided in Fig. 2. The numbers in parentheses represent the number of messages that can be transmitted during the given time interval. The schedule is created for one week, four messages can be sent in a single PC_S, while 10 messages can be sent in a single UC_S. There are 10 time slots for planned communication in PC_PART of each segment and only two time slots for unplanned communication in UC_PART of the segment. During the week, there is a possibility to send 302400 messages in total, divided into 5040 segments. Thus, there are two thirds of the time reserved for planned communication and one third for unplanned communication in the illustrated schedule.

The proposed SCPP control protocol enables the following key functions:

- *Time slot reservation* – enables the end device to request for assignment of a reserved time slot for planned communication.
- *Time slot revocation* – enables the AP or end devices to cancel the reservation of PC_S.
- *Planned data transmission* – enables the end device to send periodically repeated communication during the reserved time slots.
- *Unplanned data transmission* – enables to send communication that could not be planned.
- *Time synchronization* – enables the AP to synchronize the time of end devices using the periodic synchronization beacons.
- *Parameters propagation* – enables the AP to inform end device about currently used SCPP parameters or their modification due to adjustment to current state of the network.

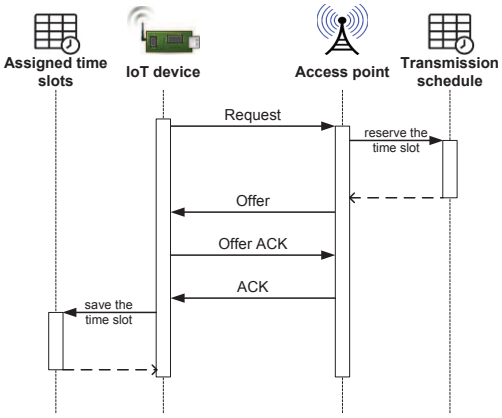

Fig. 3. The time-slot reservation process.

A. Time Slot Reservation

SCPP defines five messages to accomplish the time-slot reservation process, namely Request, Offer, Reject, Offer ACK, and ACK. This process is illustrated in Fig. 3. Firstly, the IoT end device sends the Request message to the AP, which includes expected traffic characteristics, such as the data size and the required periodicity. Based on this information, the AP allocates suitable time slots in the transmission schedule and notifies the end device about the reserved time slot using the Offer message. If the AP cannot find any suitable time slot, it sends the Reject message to the end device. Upon receiving the Offer message, the end device acknowledges the reception by sending the Offer ACK message. If the Offer message is not received within a predefined time frame, the Request message is resend after an exponential back-off time. The AP also acknowledges the reception of the Offer ACK message using the ACK message, which ends the time-slot reservation process.

B. Time Slot Revocation

SCPP defines two messages for the time-slot revocation process, namely Cancel Lease and Cancel ACK. This process is illustrated in Fig. 4. The initiator of revocation procedure (the AP or IoT end device) starts the process by sending the Cancel Lease message, which contains the identifier of the PC_S to be unreserved and the corresponding end device (to which it was assigned in the schedule). The initiator then deletes the time-slot assignment from the database. Upon reception of the Cancel Lease message, the recipient also deletes the time-slot assignment from its database and confirms the time-slot revocation by sending the Cancel ACK message. An end device can revoke only the time slots assigned to it (i.e. reserved for this end device). To increase the reliability, the Cancel Lease message is retransmitted after back-off time, if the Cancel ACK not received in the predefined time. The time slots can be also freed (i.e. reservation canceled) if the assigned end device does not use them for predefined number of times (i.e. the end device is out of range, damaged, or turned off). Such a revocation however must be allowed in the network.

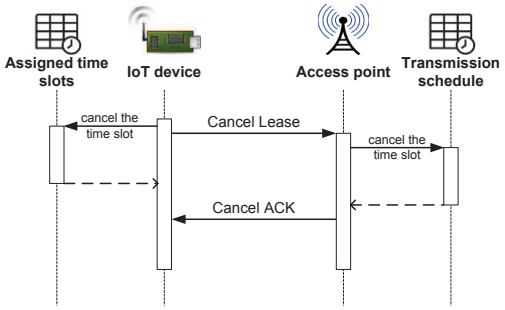

Fig. 4. The time-slot revocation process.

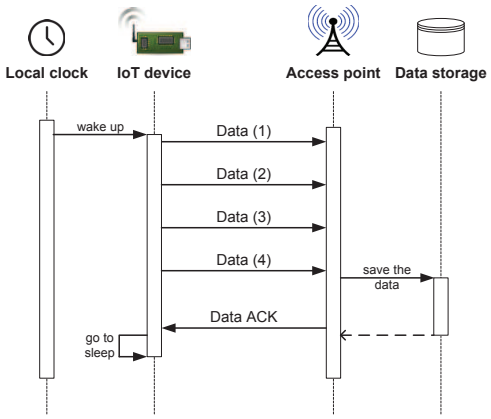

Fig. 5. The planned data-transmission process.

C. Data Transmission

SCPP defines two messages for a data transmission, namely Data and Data ACK. This process is illustrated in Fig. 5. After the sensor device measures the required parameters, it can be put to sleep (to save the energy) if another processing not required. It can wake up just before its assigned time slot for planned communication to send the measured data using the Data message (or multiple messages). After the AP receives the data, it processes them further (e.g. stores, aggregates, or forwards). If a reliable delivery is required in the network, the AP sends the Data ACK message to acknowledge the correct reception of the data. If the end device does not receive the Data ACK message for the predefined time, it assumes the data were lost and retransmits them in the slots for unplanned communication or the next assigned reserved slot (if the cumulative data size, i.e. retransmitted data and new data, is able to be transferred in the assigned slot).

D. Time Synchronization

For time-slot based functioning of the proposed SCPP, a proper synchronization in the network is inevitable. SCPP defines the Time-Sync Beacon message to accomplish this process (illustrated in Fig. 6), which contains information about the current time in the network. This message is periodically sent by the AP, which uses the Internet connection to keep its clock synchronized. End devices do not need to receive and process each synchronization message. Each end IoT device has a preconfigured time interval, in which it should

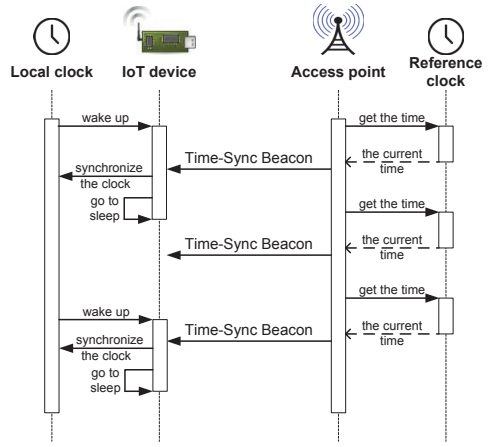

Fig. 6. The time-synchronization process.

synchronize its clock (based on the accuracy of the integrated crystal oscillator). The Time-Sync Beacon message includes also a protocol-parameters revision number, which is utilized for the parameters propagation.

E. Parameters Propagation

A propagation of the SCPP parameters enables to adjust the communication (such as the size of time slots, or the number of slots in planned and unplanned part of the segment) according to the current traffic characteristics and state of the IoT network, and thus keep a high efficiency of the protocol. For example, when newly created network has a small number of periodically communicating sensor devices, it would be inefficient to reserve a large part of the segment for planned communication. The parameters propagation enables to gradually increase the planned part, when the number of IoT devices (communicating periodically) increases. For parameters propagation, the AP periodically sends the Protocol-Parameters Beacon message (in the predefined time interval), which contains information about changed SCPP parameters. In a case that no parameter has been changed since the last beacon message, a message without parameters is sent. In another predefined time interval (less frequent than the previous), the beacon with all parameters that have non-default value is sent. It enables to synchronize the parameters for new devices that recently connected to the network (i.e. do not know the current parameters values). If a new end device recognizes the value of 0 in the protocol-parameters revision number of the Time-Sync Beacon message, it does not need to wait for Protocol-Parameters Beacon message. Another usage is the synchronization of devices that did not received some of the parameters update messages.

III. Results

The proposed collision-prevention method using the SCPP protocol has been evaluated by its comparison to existing techniques used in Sigfox and LoRaWAN IoT networks. The communication efficiency in various simulated scenarios was monitored to properly make the conclusions. The implemented

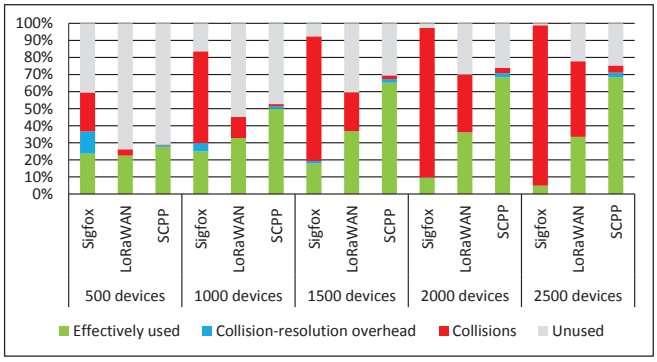

Fig. 7. Bandwidth utilization of the simulated collision-resolution techniques.

TABLE I
Comparison of the Successfulness of Transmission

Number of devices	Sigfox	LoRaWAN	SCPP
500	40.57%	74.25%	97.27%
1000	17.47%	56.40%	94.97%
1500	6.64%	40.71%	92.77%
2000	2.69%	29.96%	90.48%
2500	1.09%	22.26%	87.28%

simulator used for evaluation is turn-based, so it enabled faster simulation execution (i.e. communication for a week was simulated in few hours) and examination of scenarios that would bee too resource-intensive for a real-time execution (e.g. many IoT nodes). A simulation scenario is defined by multiple parameters, such as the simulation length (i.e. length of the simulated time), the size of planning interval (i.e. a basic structure in the transmission schedule to be planned), the number of IoT devices, or the periodicity of transmissions.

In the first scenario, the network speed was set to 100 b/s (i.e. one message per two seconds), the simulation length of one week was used (i.e. maximal capacity of 302,400 messages), the planned communication occupied 92% of time (i.e. one message per hour for each device), and the unplanned communication occupied remaining 8% of time (i.e. two messages per day for each device). Five variants of 500, 1000, 1500, 2000, and 2500 end IoT devices were simulated. All devices started simultaneously in the simulation, which represents the worst case for the proposed SCPP protocol. Fig. 7 illustrates the results of bandwidth utilization for the three collision-resolution techniques. The green color represents the effectively used bandwidth – i.e. the AP successfully received the message. The blue color represents the collision-resolution overhead – i.e. the control (in case of SCPP) or redundant (in case of Sigfox) messages were received by the AP. The red color represents the collisions – i.e. multiple devices tried to transmit a message simultaneously. The grey color represents the unused bandwidth – i.e. no messages were transmitted during those simulation turns.

Table I contains results about the final successfulness of transmission, computed as a ratio of the number of all data messages received by the AP and the number of all messages transmitted by the end devices.

The results show that with an increasing number of IoT

TABLE II
COMPARISON OF THE COMMUNICATION EFFICIENCY

Number of devices	Sigfox	LoRaWAN	SCPP
10	100.00%	99.40%	98.97%
20	99.99%	98.60%	99.31%
30	99.95%	97.03%	99.28%
50	99.60%	97.68%	99.08%
100	99.23%	94.55%	98.88%
150	98.27%	91.70%	98.78%
200	95.13%	88.72%	98.68%
250	94.70%	85.62%	98.17%

devices, the collisions grows rapidly using Sigfox and LoRaWAN based collision-resolution techniques, while SCPP keeps the collisions in a small amount (4.2% of bandwidth for 2500 devices at maximum). The proposed SCPP technique also achieved the highest amount of effectively used bandwidth and the highest successfulness of transmission in all simulation-scenario variants (with rising number of devices, the difference between SCPP and other two techniques is increasing). As one can notice, the effectively used bandwidth of SCPP stopped increasing at approximately 68% for communication of more than 1500 devices, because the planned slots in the transmission schedule were exhausted. Even so, SCPP maintained collisions at minimum and relatively high successfulness of transmission.

This experiment has shown SCPP efficiency for a relatively high number of end IoT devices. In order to determine the lower bound in the number of devices, at which it becomes more efficient than the other two techniques, we have executed another experiment using a different simulation scenario. In this scenario, a smaller number of end devices were simulated (from 10 to 250 devices) and the simulation length of one month was used (i.e. maximal capacity of 1,209,600 messages). Other parameters were the same as in the previous scenario. The communication efficiency was monitored as a ratio of the number of successfully transmitted unique data messages and the number of transmitted messages in ideal solution (i.e. without collisions, without overhead, without convergence). To illustrate a difference between the communication efficiency and the previously used successfulness of transmission, we use an example: If an IoT device in Sigfox network wants to transmit two unique data messages, it sends six messages in total (including the redundant messages). If only one message is successfully delivered, it represents transmission successfulness of 16.6% (one received message from six transmitted), however, the communication efficiency is 50% (one received message from two unique transmitted messages). The results of this simulation scenario are provided in Table II.

The results show that for the smallest number of devices, Sigfox achieves the highest communication efficiency (due to very small probability of collisions of all three redundant messages for a single unique data message). SCPP is inefficient for a smaller number of devices due to the convergence overhead of the planning mechanism. SCPP outperforms LoRaWAN technique in the simulation-scenario variants of above approximately 15 end devices and it outperforms Sigfox

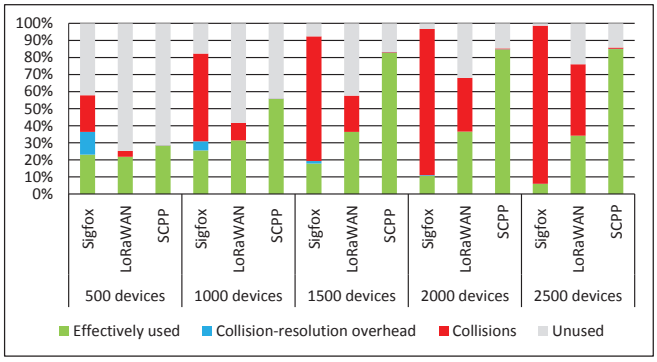

Fig. 8. Bandwidth utilization of the simulated collision-resolution techniques for a more realistic scenario.

TABLE III
COMPARISON OF THE SUCCESSFULNESS OF TRANSMISSION FOR A MORE REALISTIC SCENARIO

Number of devices	Sigfox	LoRaWAN	SCPP
500	42.10%	75.20%	99.46%
1000	17.90%	58.30%	99.25%
1500	7.50%	40.70%	98.99%
2000	3.20%	32.10%	98.56%
2500	1.40%	23.90%	98.01%

communication efficiency when more than approximately 125 end devices are used in the network. However, the difference between Sigfox and SCPP efficiency is quite small (about 1%) in case of 10 end devices (Sigfox is the most efficient), but significantly higher (about 3.5%) in case of 250 devices (SCPP is the most efficient).

In the next scenario, a more realistic network communication was simulated. Some of the devices have already been converged (the time slots assigned) and some devices started communicating during the simulation. Similarly to the first scenario, the five variants were simulated (from 500 to 2500 devices). The same scenario parameters were used with a few exceptions. 10% of the devices were dynamically randomly added to the simulation during the execution, the rest of the devices were converged at the simulation start. The average amount of planned and unplanned communication remained the same (i.e. one planned message per hour and two unplanned messages per day for each device). However, the number of slots for SCPP control messages was decreased (i.e. more planned communication could be transmitted). The bandwidth-utilization results are illustrated in Fig. 8 and the successfulness of transmission in Table III.

The results for Sigfox and LoRaWAN are very similar to the first scenario. However, SCPP achieved better results in this scenario (the effectively used bandwidth as well as the transmission successfulness). For example, in case of 2500 devices, the effectively used bandwidth was increased from 68.5% (in the first scenario) to 84.94% (in this scenario), and the successfulness of transmission from 87.3% to 98%. The main reason was fewer simultaneously converging IoT devices, which accelerated the convergence time of new devices and reduced the amount of collisions in slots for unplanned communication. The next reason is also the increased number

TABLE IV
IMPACT OF VARIOUS TIME-SLOT SIZES AND PERIODICITY ON THE SCPP EFFICIENCY

Number of devices	Effectively used bandwidth	Collision-resolution overhead	Collisions	Unused	Transmission successfulness
500	+1.92%	0.00%	−0.01%	−1.90%	+0.05%
1000	−10.24%	−0.02%	+0.01%	+10.24%	−0.19%
1500	−15.59%	−0.01%	−0.03%	+15.63%	−0.12%
2000	+0.04%	0.00%	−0.01%	−0.03%	+0.03%
2500	+0.01%	0.00%	0.00%	−0.02%	−0.04%

TABLE V
ADVANTAGES AND DISADVANTAGES OF THE PROPOSED COLLISION-PREVENTION MECHANISM

Advantages	Disadvantages
a reduced number of collisions	the increased complexity
a reduced number of retransmissions	the increased control overhead
the increased energy efficiency	the AP represents a single point of failure
the increased communication efficiency	benefits limited to periodic transmissions
the increased quality of service	benefits limited to a higher number of end IoT devices
the increased scalability	

of slots for planned communication, which was enabled by reduction of slots for control messages (since fewer devices were expected to converge simultaneously).

The last simulation scenario was targeted towards determination of an impact of various time-slot sizes and various communication periodicities on the communication efficiency using SCPP. The scenario parameters were the same as in previous scenario; however, three groups of IoT devices were created that transmitted four messages each four hours (70% of devices), eight messages each eight hours (20% of devices), and twelve messages each twelve hours (10% of devices), respectively. The values were selected in such a way that it was impossible to ideally fill the transmission schedule (i.e. without fragments). A comparison of SCPP results from this simulation scenario and the previous scenario are provided in Table IV.

The results show that for 500 devices, the effectively used bandwidth was approximately the same than in the previous scenario. The reason is that there was enough available time slots in the transmission schedule to be assigned. However, we can see that in cases of 1000 and 1500 devices, the effectively used bandwidth is smaller than in the previous scenario. The reason is less efficient utilization of the transmission schedule (i.e. a high fragmentation). In variants of 2000 and 2500 devices, the effectively used bandwidth is again approximately the same than in the previous scenario. The reason is that there was a higher number of smaller time slots allocated, which filled the gaps in the transmission schedule. The successfulness of transmission was approximately the same as in the previous scenario in all variants. Thus, the various sizes of time slots and different periodicity of planned communication have negligible impact on the transmission successfulness; however, they have relatively high impact on the effective utilization of the bandwidth.

IV. DISCUSSION

The advantages and disadvantages of the proposed SCPP collision-prevention method are summarized in Table V.

The experiments have shown that the proposed SCPP collision-prevention mechanism is more efficient (in terms of dealing with the collisions problem) than the used collision-resolution techniques in the Sigfox and LoRaWAN communication, when the number of devices is rapidly increased. The maximization of effectively used bandwidth and reduction of collisions eliminates otherwise wasted bandwidth, which would block other communication and increase the amount of collisions. This would result in lost data or a higher amount of retransmissions, which wastes the energy (undesirable for energy-constrained IoT devices). It has been also shown that the low-power long-range networks using the proposed SCPP-based planning mechanism are much more scalable, which is especially crucial if the predicted number of communicating IoT devices becomes true.

However, it must be noted that for a very low number of IoT end devices, the Sigfox collision-resolution technique was the most efficient solution. Another advantage of the Sigfox solution is its simplicity. Nevertheless, the redundant transmission of the same message can be also considered as a disadvantage, since it wastes the energy. For IoT devices with a very constrained energy source, when the energy efficiency is more important than the communication efficiency, LoRaWAN can be considered as a better alternative. For a higher number of devices, the proposed SCPP solution outperforms both of them. However, it must be also noted that SCPP is a more complex solution and the provider should consider also the implementation costs. Therefore, it is suitable for networks with a significantly high amount of connected IoT devices.

In the experiments, it has been also shown that a time-slot size and a transmission periodicity have significant impact on the effective bandwidth utilization. This problem can be alleviated by a time-slot fragmentation (using the Fragmentation Enabled flag in the Request message), which enables splitting larger slots into multiple smaller slots that are easier to fit into small gaps in the transmission schedule. Another possibility to optimize the solution is a periodic reorganization of the transmission schedule by the AP; however, the provider must

be aware of a higher amount of control traffic produced by the SCPP in such a case.

The proposed approach introduces some sort of time-division multiplexing; however, there are some significant differences. The proposed planning mechanism does not modify the medium-access method of the used communication technology (e.g. Sigfox, LoRa), but rather controls communication from the application layer. It even combines the non-competition for medium (in planned communication slots) with the competition for medium (in unplanned communication slots). It also provides a heterogeneous access, when some device can reserve a single slot with some periodicity and another device can reserve multiple slots with various periodicities according to its needs. The proposed approach is also adaptive, i.e. the sizes of planned and unplanned parts in the transmission schedule change according to the current characteristics of the network. These are also the biggest advantages and differences of the proposed planning mechanism compared to the existing solutions, which mostly target medium access layer of a specific technology.

V. Conclusion

The highly efficient techniques dealing with the collisions by listening to the communication channel cannot be reliably used in long-range wireless IoT networks. In such networks, simple techniques to increase the delivery probability are used, such as a message acknowledgement or a redundant transmission. We find these techniques as not effective enough to resolve collisions, when considering the expected growth of the number of connected IoT devices. We have proposed a new and more efficient collision-prevention technique, which is based on the new protocol SCPP to plan the communication, and thus avoid simultaneous transmissions. It especially targets IoT devices with periodic transmissions of the sensed data via long-range network access points. As experimentally shown, the result of communication planning is the reduced number of collisions, more effectively used bandwidth, fewer retransmissions, and thus higher energy efficiency (especially useful for energy-constrained IoT sensor end devices). However, all at a price of the increased complexity of the solution.

As a next step, the experiments using hardware devices will be executed to confirm the benefits of the proposed planning mechanism. However, a high number of devices will be needed to properly test the approach. The scheduling algorithm running on the access point can be further optimized by analyzing existing resource-scheduling approaches and selecting the optimal one (it was outside of this work). Also, the access point currently represents a single point of failure. Therefore, in further work, this issue will be targeted by introducing the redundancy to increase reliability and robustness of the network.

References

[1] J. Pullmann and D. Macko, "Increasing energy efficiency by minimizing collisions in long-range IoT networks," in *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*. IEEE, 2019, pp. 178–181.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[4] N. Saleh, A. Kassem, and A. M. Haidar, "Energy-efficient architecture for wireless sensor networks in healthcare applications," *IEEE Access*, vol. 6, pp. 6478–6486, 2018.

[5] M. Luvisotto, F. Tramarin, L. Vangelista, and S. Vitturi, "On the use of LoRaWAN for indoor industrial IoT applications," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[6] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 812–837, 2018.

[7] A. Hassebo, M. Obaidat, and M. Ali, "Commercial 4G LTE cellular networks for supporting emerging IoT applications," in *2018 Advances in Science and Engineering Technology International Conferences (ASET)*. IEEE, 2018, pp. 1–6.

[8] A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, and B. B. Gupta, "Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings," *Future Generation Computer Systems*, vol. 82, pp. 349–357, 2018.

[9] P. Newman. (2019) IoT report: How Internet of Things technology growth is reaching mainstream companies and consumers. [Online]. Available: https://www.businessinsider.com/internet-of-things-report

[10] Cisco. (2016) Internet of Things: At a glance. [Online]. Available: www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf

[11] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. Leung, and Y. L. Guan, "Wireless energy harvesting for the Internet of Things," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 102–108, 2015.

[12] G. Ferre, "Collision and packet loss analysis in a LoRaWAN network," in *2017 25th European Signal Processing Conference (EUSIPCO)*. IEEE, 2017, pp. 2586–2590.

[13] L. Krupka, L. Vojtech, and M. Neruda, "The issue of LPWAN technology coexistence in IoT environment," in *2016 17th International Conference on Mechatronics-Mechatronika (ME)*. IEEE, 2016, pp. 1–8.

[14] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovács, P. Mogensen, and M. Sorensen, "Coverage and capacity analysis of Sigfox, LoRa, GPRS, and NB-IoT," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*. IEEE, 2017, pp. 1–5.

[15] G. Margelis, R. Piechocki, D. Kaleshi, and P. Thomas, "Low throughput networks for the IoT: Lessons learned from industrial implementations," in *2015 IEEE 2nd world forum on internet of things (WF-IoT)*. IEEE, 2015, pp. 181–186.

[16] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 34–40, 2017.

[17] R. Piyare, A. L. Murphy, M. Magno, and L. Benini, "On-demand TDMA for energy efficient data collection with LoRa and wake-up receiver," in *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2018, pp. 1–4.

[18] R. Piyare, A. Murphy, M. Magno, and L. Benini, "On-demand LoRa: Asynchronous TDMA for energy efficient and low latency communication in IoT," *Sensors*, vol. 18, no. 11, p. 3718, 2018.

[19] L. Bhatia, I. Tomić, and J. A. McCann, "LPWA-MAC: A low power wide area network MAC protocol for cyber-physical systems," in *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*. ACM, 2018, pp. 361–362.

[20] C.-J. M. Liang, N. B. Priyantha, J. Liu, and A. Terzis, "Surviving Wi-Fi interference in low power ZigBee networks," in *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*. ACM, 2010, pp. 309–322.

[21] H.-H. Choi, H. Lee, S. Kim, and I.-H. Lee, "Throughput analysis and optimization of distributed collision detection protocols in dense wireless local area networks," *Journal of Communications and Networks*, vol. 18, no. 3, pp. 502–512, June 2016.

[22] T. A. Al-Janabi and H. S. Al-Raweshidy, "An energy efficient hybrid MAC protocol with dynamic sleep-based scheduling for high density IoT networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2273–2287, 2019.

[23] P. Gočal and D. Macko, "EEMIP: Energy-efficient communication using timing channels and prioritization in ZigBee," *Sensors*, vol. 19, no. 10, p. 2246, 2019.

[24] Sigfox. (2019) Discover how you can benefit from Sigfox technology to disrupt your industry. [Online]. Available: https://www.sigfox.com/en/use-cases

[25] Semtech. (2019) LoRa technology is connecting our smart planet. [Online]. Available: https://www.semtech.com/lora/lora-applications