Increasing Energy Efficiency by Minimizing Collisions in Long-Range IoT Networks

Jakub Pullmann, Dominik Macko
Faculty of Informatics and Information Technologies
Slovak University of Technology
Bratislava, Slovakia
Email: xpullmann@stuba.sk, dominik.macko@stuba.sk

***Abstract*—This paper is focused on increasing communication efficiency of IoT devices by minimizing collisions. We have analysed the existing collision-resolution techniques and used the acquired knowledge to specify a new collision-resolution technique. The proposal consists of a communication protocol for low speed, long range IoT networks with a large number of IoT sensors. The Access Point enables planning of periodically repeated communication into timeslots, which are organized in the transmission timetable. For each timeslot, only one IoT device is assigned to send data. This approach results in collision reduction, which leads to lower power consumption of IoT End Devices.**

***Keywords*—energy efficiency; Internet of Things; long-range networks; low-power communication; wireless sensor networks**

I. Introduction

The Internet of Things (IoT) poses a next step in the evolution of the Internet bringing new possibilities for collecting, analysing and distributing data, which allows us to create new information and knowledge [1]. Nowadays, IoT Devices are used in many areas like healthcare, education, transport, smart cities, trade, energetics, etc [2]. These areas provide a lot of various use cases for IoT Devices (health monitoring, traffic management, smart parking, etc.). In 2017 the number of IoT devices was estimated to 9 billion, which should increase to 64 billion by 2025 [3].

Low power consumption is one of the most important priorities for the majority of IoT devices. These IoT devices are often not connected to the electrical grid because of the need for flexibility or other reasons, which force usage of batteries or other alternative power sources (e.g. energy harvesting) [4]. These alternative power sources provide lower power output and complicated maintenance with higher costs. This creates motivation to reduce power consumption of IoT devices as much as possible.

There are many wireless communication technologies used by IoT devices e.g. LoRaWAN, Sigfox, ZigBee, WiFi-ah, Z-Wave, Thread, Bluetooth Low Energy, etc., which differs in various characteristics like speed, range, used frequencies, power consumption, etc. Wireless communication of IoT Devices is prone to collisions, which are basically the result of multiple devices transmitting data at exactly the same time. In such a case, transmitted data are lost and retransmission follows. This results in higher energy consumption of IoT devices and reduced throughput of the IoT network [5], [6].

There are various factors that affects probability of a collision, such as the transmission speed, the size of transmitted data, the number of devices, or the time on air [7]. The number of devices connected to IoT networks is significantly higher compared to standard networks, which makes constantly growing IoT networks more vulnerable against collision. Existing collision-resolution techniques used in IoT networks are more closely described in Section II.

In this paper, we focused on long-range wireless IoT networks, with low network speeds and centralized communication through network Access Points (Sigfox, LoRaWAN). We also focused on IoT devices with periodically repeated communication (various IoT sensors). The most effective collision-resolution technique uses detection of collisions by listening of transmission channel. Unfortunately, this approach can't be reliably used in long-range wireless IoT networks due to various problems (hidden node problem, environment interference, etc.). For these types of networks, we consider analysed collision-resolution techniques as not effective enough, which was the motivation for development of a new, more effective collision-resolution technique. Network Communication Simulator was developed to test an implementation of the proposed protocol. After completion, it will also make possible to compare this approach with the existing collision-resolution techniques.

The paper is organized as follows. In Section II, the existing solutions are described. Section III includes the proposed planning method along with the corresponding control protocol. The experimental results are outlined in Section IV, and Section V concludes the paper.

II. Related Works

In this section, we analysed collision-resolution techniques for wireless communication used in existing IoT technologies or published in research papers.

This work was partially supported 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), and the project "University Science Park of STU Bratislava" (ITMS 26240220084), co-funded by the European Regional Development Fund.

This is an accepted version of the paper:
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), 2019, pp. 178-181.
doi: 10.1109/TSP.2019.8768844
URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8768844

The collision-resolution technique used in Sigfox is very simple [8]. Device doesn't check availability of medium before transmission. Each message is transmitted 3 times, at 3 randomly chosen frequencies, in 3 different time intervals. This approach increases probability of successful transmission, which could be negatively affected by collisions or environmental interference. The main drawbacks of this method are higher power consumption caused by retransmission and higher network bandwidth consumption. It also increases probability of collision. In the case of a huge number of connected devices, it will even lower probability of successful transmission, which will make this approach counter-productive.

In LoRaWAN, a different technique is used [5]. Device also doesn't check availability of medium before transmission, but each message is send only once. After transmission, the device waits for response (ACK message). If the device doesn't receive the response, it assumes that a collision occurred. The device waits generated time interval (exponential back-off time) and then retransmits the message again. The disadvantage of this method is a need of the response message. On the other hand, compared to the technique used in Sigfox, this technique consumes less network bandwidth and performs better in the case of a huge number of connected devices.

ZigBee uses CSMA/CA, which is also used in standard Wi-Fi Networks [9]. ZigBee, unlike Sigfox and LoRaWAN, is not used for long range communication. It can efficiently use listening of the transmission channel. In this technique, the device checks availability of medium before transmission. If the medium is free, the device starts the transmission. If the medium is occupied, then the device waits generated time interval (exponential back-off time) and listens again. A collision can occur if multiple devices start to listen at the same time. In wireless networks, devices can't send and receive at the same time, so collisions can't be detected during a transmission. WCSMA/CD and CSMA/CR were proposed to face this problem. In these methods, a small listening interval is randomly chosen by each device, during which the transmission is paused and a collision can be detected. The main disadvantage of this method is problematic implementation of the small listening slot. These methods are examined in [10]. Effectiveness of the mentioned techniques (CSMA/CA, WCSMA/CD, CSMA/CR) depends heavily on reliability of listening, which is not affected only by the distance, but also by the environment interferences.

III. The Proposed Planning Method

The proposed collision-resolution technique is in the form of a communication protocol (Slot-based Communication Planning Protocol - SCPP). It is focused on IoT devices with periodically repeated communication, which is centralized through network Access Points (APs). This type of devices mostly consists of IoT sensors, with various tasks, for example, a device for monitoring Bee Hives (temperature, humidity, weight of hive, etc.). Most of the communication is sent in uplink direction (from an IoT sensor to an AP). The main advantage of this type of communication is that size, frequency, and time of transmitted data are known in advance (e.g. temperature humidity is sent every hour and weight is sent once per a day). The proposed communication protocol uses this information for planning of the communication.

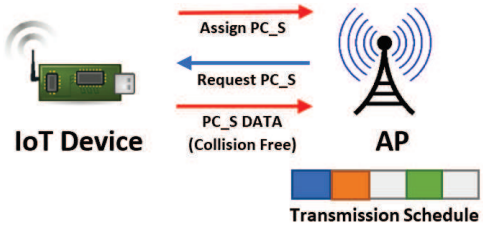

Fig. 1. The communication planning mechanism.

In SCPP, the Transmission Schedule is used. The time is divided into time slots and the communication is managed by an AP. There are two types of time slots. The first type of slots (Planned Communication Slot – PC_S) is used for sending periodically repeated communication. These slots are assigned by AP to IoT devices (End Devices/IoT Sensors) based on their request messages. Each of these slots will be assigned only to a single device, which will result in minimizing of collisions for data transmission during these slots (see Fig. 1).

The second type of slots (Non-Planned Communication Slot – NPC_S) is dedicated for other regular communication and management messages of SCPP. These slots are not assigned to specific devices and collisions can occur during these slots.

SCPP provides the following main functions:

- Reservation of Time Slots for Planned Communication
- Revocation of Time Slots for Planned Communication
- Transmission of Planned Communication
- Transmission of Non-Planned Communication
- Time Synchronization
- Protocol Parameters Propagation

These functions will be described in more detail in the following subsections.

A. The Transmission Schedule Structure

This section describes the structure of Transmission Schedule and purpose of each part. The parameters of each part (number, size, etc.) are not defined with fixed length by the protocol. This approach gives a possibility to adjust these parameters based on characteristics of each network or communication technology.

The length of the Transmission Schedule is defined as Planning Interval (e.g. one week or month), after which it repeats. It consists of a defined number of segments (see Fig. 2), which all share the same structure (see Fig. 3). Time Segment consists of a part for the planned communication (PC_PART) and a part for the non-planned communication (NPC_PART).

The part for planned communication consists of a defined number of slots (PC_S), which represents the smallest part that can be assigned by the AP to an IoT Device. During each slot, a defined number of messages can be sent (e.g. 4 messages,

Fig. 2. The Planning Interval structure.

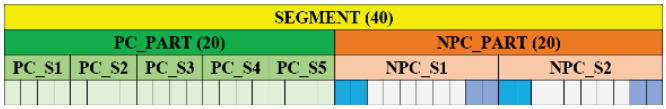

Fig. 3. The Time Segment structure.

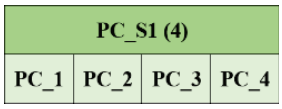

Fig. 4. The structure of a time slot for the planned communication.

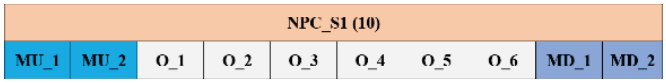

Fig. 5. The structure of a time slot for the non-planned communication.

see Fig. 4). On the assumption that all devices are working properly according to SCPP, the planned communication is collision free.

The part for non-planned communication consists of a defined number of slots (NPC_S), which are used by other regular communication (O) and management messages (uplink/downlink - MU/MD, see Fig. 5).

For higher reliability, an optional message-lost detection and retransmission is implemented for both types of communication (planned and non-planned).

B. Time Slot Reservation

SCPP uses 5 types of messages during time-slot reservation process: Request, Offer, Reject, Offer ACK and ACK.

To obtain transmission slots for planned communication, the IoT device needs to send Request message to the AP. This message contains information about planned communication (size, frequency, etc.). After receiving this message, the AP looks for a free time slot in the Transmission Schedule and responds with the Offer or Reject message. In the next step, the IoT device continues with the Offer ACK message, after which the process ends by the ACK message from the AP. To ensure reliability of this process, a retransmission of lost messages is implemented.

C. Time Slot Revocation

SCPP uses 2 types of messages during the time-slot revocation process: Cancel Lease and Cancel ACK. It can be initiated by either AP or IoT Device. The initiator starts time-slot revocation by sending of the Cancel Lease message. To confirm receiving of this message, the Cancel ACK message is sent. After this process, both devices erase the specified time from their memory. The time slot can be also revoked by reaching its expiration date.

D. Time Synchronization

For proper functioning of SCPP, the time synchronization must be used. This is accomplished by regular Time-Synch messages, which are sent by the AP to IoT devices. An IoT device doesn't need to receive each Time-Sync message. The necessary frequency of internal clock updates can be individual for each IoT device.

E. Protocol Parameters Propagation

Some of the SCPP parameters can be changed dynamically using parameters-propagation messages, which can be send by the AP in regular time intervals. This approach gives a possibility to adjust these parameters according to the current state of the IoT network, with an aim of maximizing communication efficiency. Adjusting these parameters by software or hardware updates would be slower, complicated, and expensive.

IV. Experimental Results

To evaluate the proposed protocol, a simulator of network communication was developed. It was used to compare the SCPP and other collision-resolution techniques using various communication scenarios.

The simulator provides the following main functions:

- Creation and editing of simulation scenarios
- Simulation execution
- Evaluation of simulation results

These functions are implemented by 4 main modules: Simulation Scenario, Simulation, Simulation data collector, and Evaluator (see Fig. 6).

A simulation scenario defines multiple parameters of the simulation, which affect the execution and evaluation methods of the simulation. It defines the parameters like length of simulation, size of planning interval, number of IoT devices, frequency of transmission, type of graphs in evaluation, etc.

The simulator simulates the communication between the AP and IoT devices. Data from the simulation are collected during the simulation, and later used for evaluation. The simulator is implemented as a turn-based simulator (not real-time), which enables faster execution of a simulation. It also enables to simulate scenarios that would be too performance-intensive for a real-time execution. The simulator runs as a program on a single PC, without any need of physical or virtual network cards.

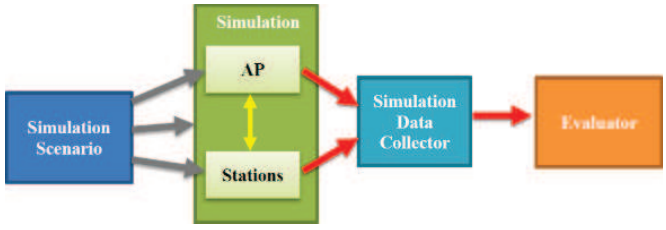

Fig. 6. The Network Simulator main modules.

A. Results and Discussion

The simulator has already been used for initial simulations and comparison. IoT devices communicated using the collision-resolution techniques like in Sigfox, LoRaWAN, and the proposed SCPP. There were three variants of simulation scenarios (for 500, 1500, and 2500 of IoT devices). The network speed was set to 100b/s (like in Sigfox) and the simulated length of the communication was set to one week (i.e. the simulation time). The simulation results in Fig. 7 illustrate the bandwidth utilization for individual scenarios. The effectively used bandwidth (green color) represents the percentage of turns in which the AP successfully received the data message. The red color represents the percentage of turns in which collisions occurred (i.e. multiple devices communicated simultaneously). The blue color illustrates an overhead of the collision-resolution technique – i.e. it represents simulation turns in which control or redundant messages were received by the AP. The rest of the bandwidth was unused – i.e. the grey color represents the percentage of turns in which no message was transmitted.

The results show that the effectively used bandwidth was approximately the same using all three communication methods for 500 devices. However, when increasing the number of devices, the amount of collisions increased rapidly using Sigfox and LoRaWAN based collision-resolution techniques. There is only a small amount of collisions using SCPP (due to the non-planed communication), even for 2500 devices. However, further examinations are required to state the higher bound of the number of devices creating the collision-free environment in various scenarios (e.g. various transmission intervals, various numbers of devices). It means, we need to investigate how many devices can communicate using the proposed method without any collisions (or with a sufficiently low amount of collisions). The low-power long-range networks using the proposed planning method should be much more scalable than those using only the existing medium-access and collision-resolution techniques. And this is especially important when considering the expected number of connected IoT devices in the forthcoming years.

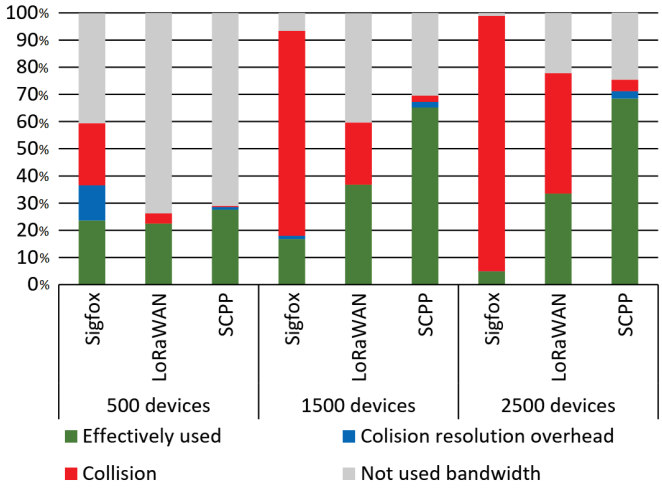

Fig. 7. Initial comparison of the simulated collision-resolution techniques.

V. Conclusions

The collision-resolution techniques using detection of collisions by listening can't be reliably used in long-range wireless IoT networks. For these types of networks, we consider the analysed collision-resolution techniques as not effective enough. In this paper, we proposed a new, more effective collision-resolution technique in the form of communication protocol. It is focused on IoT devices with periodically repeated communication through network Access Points. Transmission Schedule with time slots is used for communication planning. For each timeslot, only one IoT device is assigned to send data, which results in collision reduction, fewer retransmissions, and thus lower energy consumption of IoT End Devices. This enables to prolong the lifetime of such devices or to incorporate more functions into a device with the same power source.

The Network Communication Simulator was developed to compare the proposed protocol with other collision-resolution techniques used in low-power long-range IoT networks. The initial simulations indicate that the number of collisions is rapidly reduced using the proposed method when scaling the amount of end devices. However, further testing and evaluation using multiple scenarios with various simulation parameters need to be taken in order to properly prove the promising benefits of the proposed SCPP method.

References

[1] M. Jadoul. (2015) The IoT: The next step in internet evolution. [Online]. Available: https://www.nokia.com/blog/iot-next-step-internet-evolution/

[2] 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.

[3] 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

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.