Year: 2019

Scalable Transport Mechanisms for Blockchain IoT Applications

Schiller, Eryk ; Rafati Niya, Sina ; Surbeck, Timo ; Stiller, Burkhard

Abstract: This paper studies various methods that improve the performance of Blockchain systems integrated with the Internet of Things (BIoT) using the LoRaWAN access method. Duty Cycle Enforcement (DCE) and Listen Before Talk (LBT) mechanisms as the channel access methods, Automatic Repeat reQuest (ARQ) on the Transport Layer, and transaction aggregation on the Application Layer are evaluated. The main focus is put on the system performance studying the maximal number of transactions submitted, reliability of transport schemes, and the energy efficiency of the BIoT system. The combination of LBT-based MAC, the ARQ-enabled Transport Layer, and transaction aggregation at the Application Layer provides a good trade-off between submitted transaction count, packet loss, and energy efficiency. The proposed scheme complies to the data integrity demands of BIoT applications by specifying a reliable data transmission scheme from IoT devices to the BC.

DOI: https://doi.org/10.1109/LCNSymposium47956.2019.9000673

Originally published at:
Schiller, Eryk; Rafati Niya, Sina; Surbeck, Timo; Stiller, Burkhard (2019). Scalable Transport Mechanisms for Blockchain IoT Applications. In: 44th IEEE Conference on Local Computer Networks (LCN 2019), Osnabrück, Germany, 14 October 2019 - 17 October 2019, IEEE.
DOI: https://doi.org/10.1109/LCNSymposium47956.2019.9000673

Scalable Transport Mechanisms for Blockchain IoT Applications

Eryk Schiller, Sina Rafati Niya, Timo Surbeck, Burkhard Stiller
Communication Systems Group CSG@IfI, University of Zürich
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
Emails: [schiller|rafati|stiller@ifi.uzh.ch], timo.surbeck@uzh.ch

Abstract—**This paper studies various methods that improve the performance of Blockchain systems integrated with the Internet of Things (BIoT) using the LoRaWAN access method. Duty Cycle Enforcement (DCE) and Listen Before Talk (LBT) mechanisms as the channel access methods, Automatic Repeat reQuest (ARQ) on the Transport Layer, and transaction aggregation on the Application Layer are evaluated. The main focus is put on the system performance studying the maximal number of transactions submitted, reliability of transport schemes, and the energy efficiency of the BIoT system. The combination of LBT-based MAC, the ARQ-enabled Transport Layer, and transaction aggregation at the Application Layer provides a good trade-off between submitted transaction count, packet loss, and energy efficiency. The proposed scheme complies to the data integrity demands of BIoT applications by specifying a reliable data transmission scheme from IoT devices to the BC.**

I. Introduction

Blockchains (BCs) provide decentralized data storage for general Information Technology (IT) systems. BCs were introduced at the end of 2008 and serve as a platform for secure and anonymous transactions processing using a decentralized network of regular computers. Typically, BCs are constructed as a linked list of data blocks, in which changing a single bit in any of the previously stored blocks can be immediately discovered by participating peers. In BCs, miners are main actors that verify the validity of stored data.

IoT-integrated use cases have raised a high attention in the past decade [18], as supply chain monitoring, environmental monitoring, smart cities, smart industries, and healthcare focus on data immutability and require IoT systems for measurements, data collection, and active control. Thus, the integration of BCs and IoT into BIoT-supportive applications responds to demands of persistent storage of strongly secured data, where automated data collection becomes a key for offering transparency and reliability.

A highly demanding role of BIoT applications requires an elaboration and analysis of underlying IoT protocols, which form the communication basis for IoT systems. Thus, the studies on the range of communication, data rates, maximum transmission units (MTUs), reliability of communication protocol, and the energy efficiency are required to appropriately support IoT deployments [18]. To understand the requirements of BIoT systems, prototype BIoT applications were developed and analyzed in the context of Low Power Wide Area Networks (LPWAN), where specifically Long Range (LoRa) Wide Area Network (WAN), Sigfox, IngenuRPMA, Weightless-N, Long Term Evolution (LTE) Machine Type Communication (MTC), *i.e.,* LTE Cat-M or Narrowband-IoT (NB-IoT) communication technologies are currently under deployment [20], [26].

LoRa offers long-range communication and low power consumption. LoRa is a communication technology designed for lightweight IoT devices [1]. LoRa defines a radio layer based on the Chirp Spread Spectrum (CSS) modulation. The LoRa operation depends on Bandwidth (BW), Spreading Factor (SF), and Coding Rate (CR). The CSS modulation developed in LoRa provides low reception sensitivity allowing for transmissions over long distances. It lets end devices to communicate within a range of several kilometers outdoors and hundreds of meters indoors [30]; some sources report about successful transmissions over 100 km LoRa links[1].

LoRaWAN defines a radio access method [28] similar to ALOHA [12]. To send data, a device *wakes up* and immediately transmits a packet over the air to surrounding gateways; therefore no Listen Before Talk (LBT) mechanisms exist in the regular LoRa operation. The LoRa channel access method and pure ALOHA only differ in the variable packet length used in LoRa in comparison to the fixed packet size in ALOHA. LoRa operates in the license-free Industrial, Scientific and Medical (ISM) radio band. For example, in Europe, LoRa operates in the 868 MHz frequency band. The European Telecommunications Standards Institute (ETSI) regulations of the 868 MHz frequency band implement severe restrictions on the limits on the maximum Duty Cycles (DCs). DC is defined as the fraction of time, in which a device can transmit over the air, between 0.1% and 10% in the 863–870 MHz band depending on the selected sub-band, when the device does not implement any LBT mechanism.

A brief overview of LPWANs is available in Table I [24], [26]. The technologies are characterized in terms of communication range, throughput, and Medium Access Control (MAC) MTU sizes.

LoRaWAN is arguably the most adopted among current LPWAN standards. It features simple network structures, provides network management, and enables ubiquitous license-free connectivity, which is advantageous for outdoor BIoT applications [13]. It should be noted that in the cellular IoT communication such as Extended Coverage–Global System

[1] https://github.com/sandeepmistry/arduino-LoRa

TABLE I
LPWAN PERFORMANCE COMPARISON.

Technology	Communication Range	Throughput	MAC MTU (Byte)
LoRaWAN	2 – 5 km urban, 15 km suburban	0.3 to 50 kbps	256
SigFox	10 km urban, 50 km suburban	100 bps	Fixed 12
IngenuRPMA	20 – 65 km	up: 624 kbps down: 156 kbps	64
Weightless-N	5 km urban 30 km suburban	30 kbps to 100 kbps	max. 20
LTE-M	12 km	up: 1 Mbps down: 1 Mbps	1500
NB-IoT	15 km	200 kbps	1600

for Mobile Communications–Internet of Things (EC-GSM-IoT), LTE NB-IoT, and LTE MTC, devices operate in licensed frequency bands; therefore a private network cannot be instantiated without the support of a Mobile Network Operator (MNO), which is a significant disadvantage in comparison to license-free radio technologies such as LoRaWAN.

The utilization of LoRaWAN for BIoT applications comes with severe limitations especially in the scope of scalability in terms of growing payload sizes, data rates (*i.e.,* transactions per hour), and the number of supported users. The following four problems of LoRa are considered in this work:

1) The minimum MAC MTU of 55 Bytes for the 125 kHz BW and SF 12, and the maximum MAC MTU of 222 Bytes for 125 kHz BW and SF 7 communication raises the need of managing data transactions in terms of continuous data streams supporting fragmentation among small chunks of data. The BIoT transactions have to be provided among different transmissions fragmented among several packets assembled at the Network Server (NS) and delivered towards BC miners that can reside in a cloud environment.
2) Strictly limited air time leads to low transmission capacity sometimes constrained to a couple of bytes per day. Thus, the efficiency of transport mechanisms especially dealing with overhead in each packet sent impacts on the overall system performance.
3) Data integrity plays an important role in the BIoT system design. The communication between LoRa nodes and Gateways (GW) is encrypted within the LoRa network, however, data integrity has to be provided at every level of the system. Therefore, different organizations of the transaction mechanisms shall be considered. As an example, IoT devices can directly issue BC transactions assuring that legitimate information is stored in the BC under the assumption that devices are protected against tempering, controlling, and key extraction. In addition, the perception layer is secured against third-parties [21].
4) To tackle the energy efficiency the general transaction mechanism needs to be energy efficient. Since data collected by LoRa nodes has to to be sent and signed, the protocol overhead and the use of costly asymmetric key cryptography should be reduced to minimum to guarantee a long run operation of often battery powered IoT devices.

To address these 4 major issues, this work studies different mechanisms allowing for efficient BIoT data streams. The scalability and performance improvements reached by the studied methods is evaluated in the NS-3 simulator by examining wide range of IoT nodes (1-1,600) and packets sent (1-40,000) per hour.

This paper is organized in the following way. Section II discusses the related work on LPWAN protocols. Section III elaborates on the methods considered to improve the communication performance in BIoT systems. Section IV introduces the scenarios developed in the simulator; it is followed by Section V, which describes positioning of nodes and gateways in the simulation according to real data gathered from The Things Network (TTN) [10]. The simulation and evaluation of results are presented in Section VI. Finally, Section VII concludes the paper.

II. RELATED WORK

This paper studies BIoT data streams and does not describe different BC technologies in detail. It tackles the LPWANs problems for BC applications focusing on the the efficiency of communication protocols that provide high data rates and maintain low overheads. The communication methods have to guarantee high energy efficiency through reduced power consumption of IoT devices. In addition, in BIoT applications, the integrity of data needs to be assured. The remaining part of this section lists the main problems of LoRaWAN that can influence on the performance of BIoT systems.

The performance of LoRaWAN strictly follows ALOHA with the maximum channel capacity of 18% (*i.e.,* only 18% of the time is used for successful transmissions) and the increased collision ratio. As an example, for the link load of 0.48, the collision ratio is around 60% (*i.e.,* the ratio between lost packets due to interference and overall packets sent in the network) [14]. The impact of collisions is, however, significantly mitigated by the capturing effect and orthogonal spreading factors, such that some transmissions benefiting from a stronger signal are successful despite collisions. Typically, in outdoor cases, there is a loss rate of less than 10% over a distance of 2 km for SF 9-12, and more than 60% loss rate over 3.4 km for SF 12.

Depending on the DC (*i.e.,* how frequently the spectrum is used to transmit data) of LoRa devices, their lifetimes can be significantly extended. For instance, up to 17 years for a node (*i.e.,* an end-device) reporting 100 Byte once in a day [25], [27]. The pure ALOHA implementation of LoRa devices does not conform to the LBT schema required by the regulatory authorities such as ETSI. When LBT is not used, the transmitters have to obey strictly enforced maximum DC regulations. This obviously limits the throughput of devices and the overall network capacity.

The work in [13] realized that for high DC values, the network throughput is limited by collisions, as in the pure ALOHA case, whereas low DCs (*e.g.,* the maximum DC set by the ETSI regulations, *i.e.,* 0.1% - 10%) prevent devices from increasing their packet transmission rates and limit the overall throughput of the network.

The work of [30] improves the performance of LoRaWAN and do not considerably increase the energy consumption. They provide a simple LBT enhancement to LoRaWAN, which effectively lowers the collision ratio. Their results show that the Carrier Sense Multiple Access (CSMA) considerably lowers the collision ratio, while only slightly increasing energy consumption. Moreover, CSMA is implemented through an LBT mechanism preceding every transmission, therefore, the devices are relieved from restrictive ETSI DC regulations of 0.1% - 10% allowing for higher achievable throughput. Furthermore, they observed that CSMA feature significantly lowers the energy consumption in comparison to the regular LoRaWAN for a large number of devices. Finally, they significantly increase data rates as well as the probability of successful transmissions for low density networks at the expense of slightly higher energy consumption. At the same time, the probability of successful transmissions, throughput as well as energy efficiency for high density networks are improved.

[22], [23] assessed the performance of LoRaWAN. They implemented a C++ NS-3 module that simulates the complete LoRaWAN network consisting of tens of thousands of end devices. Their link model is based on the underlying sub-models:

1) Link Measurement Model: estimating the signal strength at the receiver site,
2) Building Penetration Loss Model: modeling the losses caused by external as well as internal walls of buildings,
3) Correlated Shadowing: modeling fading of the signal with various variables, *e.g.,* time, geographical position as well as radio frequency
4) Link Performance Model: modeling the reception sensitivity and signal to interference ratio taking into account partial orthogonality of spreading codes used for encoding the signal with different SFs.

[16], [17] provides modeling of LoRaWAN networks in NS-3, which consists of different elements (*i.e.,* Error Correction Encoder/Decoder, Digital Interleaver/Deinterleaver, Data Whitening/De-Whitening, Gray Encoder/Decoder, LoRa Modulator/De-Modulator as well as Additive White Gaussian Noise channel): First, an error model for the LoRa modulation was implemented in NS-3 based on base band simulations of a LoRa transceiver over an additive white Gaussian noise channel. Second, the LoRaWAN physical OSI layer (PHY) and Medium Access Control OSI (MAC) layers were added in NS-3 to represent LoRaWAN gateways and simple class A end devices [28]. Third, NS-3 applications were developed to represent the behaviour of class A end devices and gateways. Finally, a simple Network Server (NS) was added to NS-3.

[29], [30] presents an NS-3 module which simulates the behavior of LoRaWAN. To assess the module, they compared the simulation results with measurements on a real-world testbed and other measured values reported by [19]. The model description is not extensively presented in the paper, however, it is demonstrated that it correctly represents the capturing effect lowering the packet loss ratio due to collisions. The simulation of the capturing effect with orthogonal spreading factors is, however, unclear. To estimate energy consumption of battery powered end devices, the energy framework of [31] was used, which is already included in NS-3.

Based on the comparative analysis done on the related work, the simulations in this work are being developed based on the work of [22], [23]. Unfortunately, the work of [29], [30] is scarcely documented. It, however, contains the description of their efficient LBT strategy which, we integrate with the solution of [22], [23] in this work. Furthermore, this work studies the influence of LBT on the MAC layer, the Automatic Repeat reQuest (ARQ) on the transport layer (*i.e.,* note that all downstream messages in LoRa are initiated by the NS, therefore, as an end-to-end scheme, such an ARQ mechanism can be understood as a transport layer instrument), and the transaction aggregation on the application layer to provide an efficient communication scheme for BIoT application using LoRaWAN.

III. Mechanisms for Improved Performance in BIoT Applications

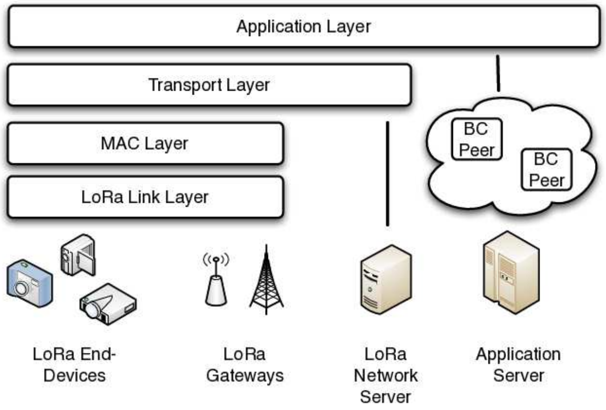

Fig. 1. The Architecture of the BIoT-enabled LoRa Network.

The architecture of the network is presented in Fig. 1. It illustrates (i) the Lora Physical and Medium Access Control layers enabling radio communication between LoRa end-devices and GWs, (ii) the Transport Layer providing data reliability mechanisms spanned between end-devices and the LoRa NS, and (iii) the Application Layer protocols supporting end-to-end transmissions between end-devices and the Application (e.g., BC peer-to-peer network).

This work studies an impact of different techniques improving performance of the BIoT-enabled LoRa network taking into consideration the 4 major issues aforementioned in Section I, *i.e.,* recovering from the packet loss, providing high reliability, and increasing the LoRa network throughput, while maintaining an energy efficient operation.

As mentioned in Section II, poor performance of the pure ALOHA channel access method in LoRa [1] can be improved by using CSMA techniques also including the LBT mechanism [30] and therefore relieving the nodes from using highly restrictive DCs and improving the overall throughput of the network. The introduction of the CSMA mechanism on the link layer should improve the overall network capacity expressed in the number of BC transactions submitted from IoT devices to a BC and has to be studied.

Modern networks detect packet losses at various levels of the system. Typical radio networks such as IEEE 802.11, IEEE 802.15.4, or LTE integrate the Automatic Repeat ReQuest (ARQ) mechanism on the link layer providing high data reliability. The purpose of the ARQ mechanism is the detection of lost segments and their re-transmission between the source and the destination. Moreover, the ARQ mechanism might be also integrated with upper layers as well. The ARQ mechanism typically resides on the transport layer, e.g., Transmission Control Protocol (TCP) and can also be integrated into the Application itself.

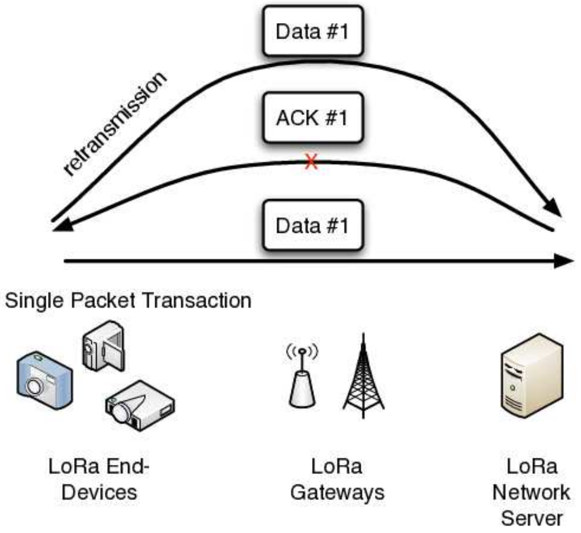

Fig. 2. The ACK Retransmission Scheme.

Packet losses can be detected by positive Acknowledgements (ACKs) confirming the reception of every data packet by the signaling ACK packets. When the source does not receive an ACK for a given data transmission, it resends the currently transmitted segment until the ACK arrives indicating a successful data transmission between the source and the destination. Therefore, the reliability of the data transmission is determined by an ACK system coupled to re-transmissions and has to be studied. This works uses downlink data transmissions between LoRa end-devices and the NS to implement an ACK retransmission scheme confirming the reception of uplink packets (*cf.* Fig. 2).

To provide data integrity, BC systems use cryptographic signatures computed over transactions submitted to the BC. High data integrity of BIoT can be provided by transactions submitted directly from IoT devices. There are two major aspects of such a design considered in this work. The size of the transaction and the cryptographic overhead of such a system. For example, if the system uses Edwards-curve Digital Signature Algorithm (EdDSA), *e.g.,* Ed25519 [15], the cryptographic signature is of size equal to 64 B. However, in some configurations (i.e., BW=125 kHz, SF=12), packets in LoRa are bound to the 55 Byte MAC MTU. Therefore, the signature has to be fragmented over two uplink messages. Considering the size of each data packet and signature, it is crucial to calculate the overall overhead in the designed scheme.

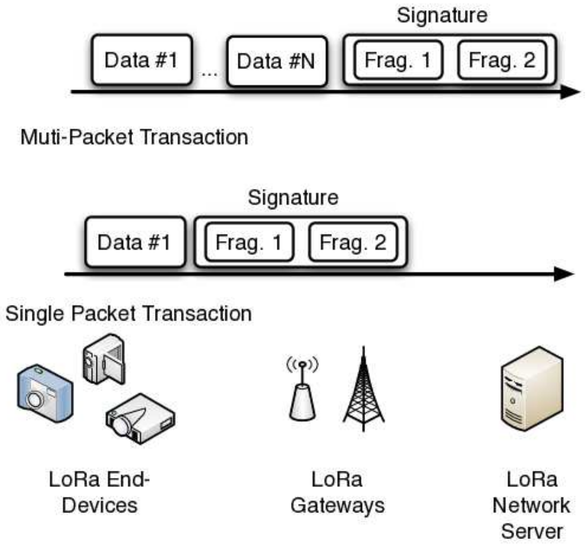

Fig. 3. The Multi-Packet Transaction Scheme.

To mitigate the overhead problem, this work proposes an aggregation scheme, where the data is signed once every N packets. The data collected by LoRa nodes, are sent within 55 Byte segments, and being signed at the end after every aggregation window. For example, in the case of N=10, 10 data packets are confirmed by a single cryptographic signature (*cf.* Fig. 3). The downside of this scheme includes elevated memory consumption, since unsigned packets have to be stored in a cache on IoT devices. Additionally, a decreased transaction delivery ratio is observed, since multiple packets have to be successfully delivered to the NS. The proposed transmission scheme follows a BC-agnostic logic, thus, can be adapted to the needs of any BC. In general, all devices can send aggregated transactions to the BC by respecting the BC-specific transaction structure.

From the energy efficiency point of view, the aforementioned methods will be studied in Section VI. First, the use of CSMA schemes implementing LBT in LoRa MAC should decrease the number of collisions providing more efficient communication. The introduction ACK on the transport layer, should detect losses at a small cost of sending tiny ACK signaling messages. Finally, the aggregation scheme should decrease the number of cryptographic signatures sent in the network, therefore reducing the channel utilization and effort spent on computing signatures.

IV. Simulation Specification

This works studies performance of the three aforementioned techniques, i.e., (1) CSMA vs. pure ALOHA on the MAC layer, (2) ACK mechanism coupled to re-transmissions vs. unconfirmed data packets on the transport layer, and (3) aggregation meaning signing multiple vs. a single packet by the application layer in a blockchain-compliant data-stream. The end-devices send multi-packet transactions signed, which are later on forwarded to a blockchain.

A. MAC Layer

The NS-3 module provided by [23] simulates physical, link layer, and network layer of LoRa and is the basic simulation environment of this work. It was also decided to extend it with the *CSMA-x* module specified by [30]. CSMA-x measures the channel during the Clear Channel Gap (CCG) window of 10 ms. If there is another detectable signal exceeding the device reception sensitivity threshold in CCG, the device needs to defer its own transmission for some period of time. [30] uses a random backoff of k seconds. The back-off time depends on the n-th re-transmission attempt and is randomly selected from the $[0, 2^{n-1}]$ interval. If, however, after n = 3 attempts, the channel is still evaluated busy, the transmission is assumed unsuccessful and cancelled. The integration of the CSMA-x mechanism by [30] with the solution of [23] allows for the simulation of both pure the ALOHA and LBT-compliant MACs.

B. ARQ on the Transport Layer

The work of [23] also allows for selecting the ARQ mechanism coupled to retransmissions. A LoRa device may receive data (*e.g.,* ACK) during two fixed-length receive-windows of 0.01 s at specified times (1 s and 2 s) after the uplink transmission. If the ACK message for a given data packet arrives, the packet is delivered. Otherwise, the nodes can schedule retransmissions. Typically, 8 retransmissions of unsuccessful packets are executed.

C. Multi-Packet Transactions

Multi-Packet Transactions adhere to the aggregation mechanism described in Section III letting every end-device transmitting signed multi-packet transactions. The Multi-Packet Transactions may also use the underlying ARQ / retransmission scheme requiring the gateway to confirm every received data chunk. When the ACK is missing, the end-device can retransmit a given missing segment up to 8 times.

This work implements the Multi-Packet Transaction traffic source as the Constant Bit Rate (CBR) mechanism. The adjustable delay between two successive multi-packet transactions is referred to as *interTransactionDelay*, while with *intraTransactionDelay*, the interval between two consecutive packet transmissions within a transaction can be adjusted. It should be mentioned, that for all multi-packet transaction scenarios simulated in the course of this work, for *interTransactionDelay* usually the same time values as for *intraTransactionDelay* were chosen.

For all the simulation scenarios, except for the efficiency-improved LBT-scenarios, the corresponding parameters of simulated devices with respect to PHY- and MAC models provided by [22], [23] are used in this work as well. The configuration of the CSMA-x protocol is identical to the work provided by [29], [30].

V. Location of LoRa Nodes

This work uses real and random locations of LoRa nodes. The freely available database provided by TTNMapper.org [11] is useful to analyze an existing LoRaWAN network. TTNMapper is a project providing a global map displaying the coverage of LoRaWAN gateways, which is part of TTN [10] that is a community-based public LoRaWAN-network.

A. Implementation Procedure

Using a Python version of the S2 geometry library [6], [7], a circular area with radius of 10 km around the city center of Zurich in Switzerland was defined. The circular shape is used for the first filtering stage based on geographical positions. Only end-devices from within this area are considered for further processing.

The second filtering stage performs analysis of each end-device's lifespan as well as of their total number of transmissions and removes those, which only existed for less than 24 h or transmitted less than 15 packets. It is assumed, that end devices (nodes), which did not pass this filtering stage, were exclusively used for testing purposes and, therefore, are not interesting for this analysis.

As the TTNMapper.org data set features geographic positions of end devices, it was decided to reuse this data as realistic input for the simulation. Therefore, the sphere-based coordinates (latitude-/ longitude) present in the data set are mapped to NS-3 metric Cartesian coordinate system. This step was accomplished by the Python-version of the PROJ.4 library [4], [5], which allows for mapping coordinates from one coordinate system to another. In this context, coordinates of the commonly known sphere-based WGS84 system [9] are mapped to the metric 2D-plane projection CH1903 [8] covering Switzerland and Liechtenstein. This implementation only focuses on devices from within a rather small area – bearing in mind the used map projection. Therefore, the converted coordinates are normalized by defining a new origin point (X, Y) = (0, 0), which is located 10 km to the south and 10 km to the east of the center of the city of Zurich.

Fig. 4 shows the geographical positions of TTN end-devices using the OpenStreetMap [3]) in the city of Zurich. As the number of nodes with known geographical positions is low in the TTNMapper data-set, we grow the number of nodes in the area by randomly locating additional LoRa nodes around discovered end-devices (i.e., providing random locations in squares having 2 km edges shaped around end-devices). In such a way, this work provides realistic locations of devices in dense and randomized scenarios as well. As the number of GWs is small, we use realistic positions for GWs received directly from the TTN data set. This will allow for a simulation of realistic interference profiles among end-devices.

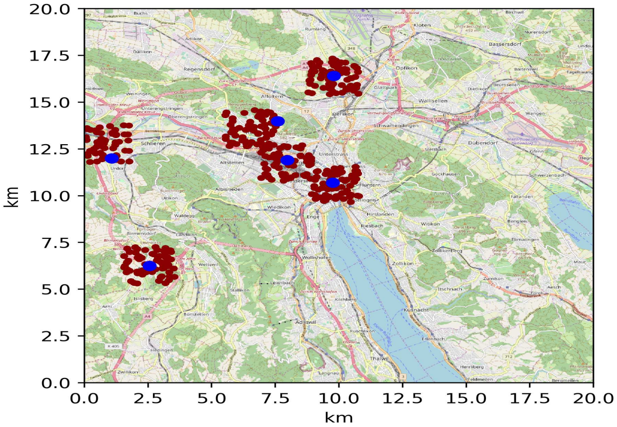

Fig. 4. Regularly Transmitting TTN Nodes in The Zurich Area.

Analysis over the entire TTNMapper.org data set [11] was conducted that resulted in the histogram (*cf.* Fig. 5) that shows the distribution of transmission periodicities among TTN end-devices. The histogram is overlaid with a kernel density curve. Using advanced FFT analyses, we discovered that majority of devices originate traffic on a regular basis using only one frequency, e.g., they provide one packet daily. Periodicities range from two hours (at index 0) up to two weeks (350 Hours).

VI. Simulation Results

The total simulation time is set to 60 min for all scenarios. This might seem low in terms of discovered transmission periodicities in Section V, however, the objective of this work is the scalability in BIoT applications having in mind high end-devices densities (*i.e.,* hundred of devices per GW) and low periodicities (*e.g.,* nodes reporting transactions having the inter-transaction delay at the level of seconds). For the conducted simulations, this is enough time for letting each end-device to transmit at least a couple Multi-Packet transactions, while keeping the simulation completion time reasonable. It is assumed that choosing longer simulation runs is not needed, as due to the steady transmission conditions, the same effects in the network repeat all over again.

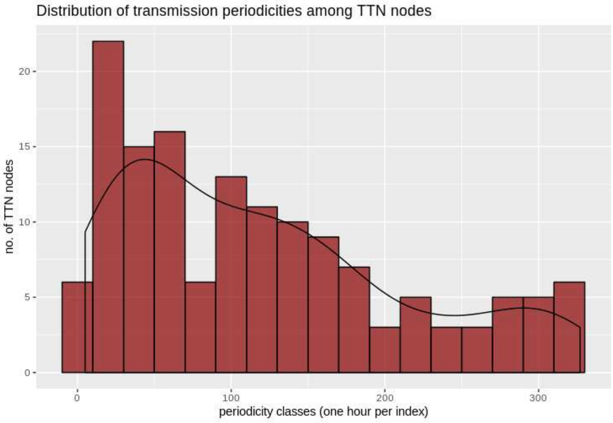

Fig. 5. Global Transmission Periodicity Histogram in TTN.

The simulation studies two MAC configurations, *i.e.,* the basic LoRaWAN class A MAC abbreviated as Duty Cycle Enforcement (DCE), and the LBT LoRaWAN MAC provided by [30] abbreviated as LBT; two Transport Layer configurations with and without the retransmission scheme coupled to ACK messages abbreviated as ACK and NOACK respectively (*cf.* Fig. 2); and the Single Data Packet transaction scheme followed by the fragmented signature denoted as $N = 1$ as well as the Multi-Packet Transaction scheme, in which $N = 10$ data packets are followed by the corresponding cryptographic signature (*cf.* Fig. 3).

The size of the data packets is equal to 42 Bytes. A BC transaction requires a signature, which is generated with the help of the Ed25519 cryptography [15]. The signature is, therefore, of size equal to 64 B and is carried in separate two packets following a transaction of size equal to 32 B each, i.e., a 64 B signature cannot be sent over the LoRa PHY BW=125 kHz, SF=12 configuration, which only allows for MAC MTUs of 55 B. Therefore, the signature was fragmented.

The number of GWs is fixed and equal to 6. This work experiments with the following end-device densities, and inter-transaction delays:

- *Inter Transaction Delay / Inter Transmission Delay*: [120, 95, 65, 35, 14, 9] s,
- *Ndevices (Number of Devices)*: [200, 400, 600, 800, 1,000, 1,200, 1,400, 1,600].

For couple hundreds end-devices and elevated traffic loads, there is considerable amount of losses. The subsequent part of this sections fixes the number of end-devices to 1000 and performs experiments with varying number of inter-transaction delays (*i.e.,* inter-data packet arrival). It is worth noting that the transactions are originated on nodes on a regular time basis, however, when the MAC layer is still delivering an old transaction (a packet) through retransmissions, a new transaction (data packet) is not generated. Even if the Application is configured to deliver a packet per a time unit, it will wait until the MAC operation for the preceding packet is finished.

The physical layer of LoRa is configured according to the appropriate transmission power and SFs so that the transmission air-time is minimized under the assumption that every end-device can reach at least one GW [22], [23]. In terms of the channel model, *LogDistancePropagationLossModel* for propagation loss and *ConstantSpeedPropagationDelayModel* for propagation delay of NS-3 [2] are used in the simulation. The LoRa module adds a 9 B MAC header; therefore the total size of data packets transmitted over the air increases respectively. The size of ACK messages on the Transport Layer is equal to 9 B.

In general, scenarios simulating transmissions of signed multi-packet transactions scored significantly lower success rates than Single Packet transaction scenarios (*cf.* Fig. 6). This is due to the fact, that for Multi-Packet transactions $N = 10$,

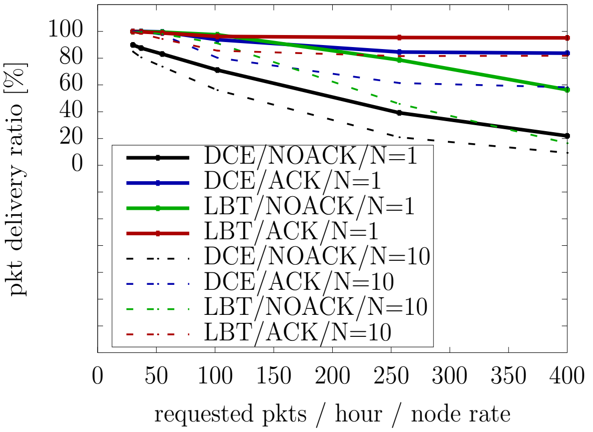

Fig. 6. Packet Loss Experienced by End-Devices, 1000 End-devices, 6 GWs.

all twelve packets belonging to a transaction (i.e., 10 data packets, and 2 signature fragments) have to be consecutively received intact, such that a transaction counts as successful, whereas a Single Packet transaction increases the success rate, while only 3 packets (1 data packet and 2 signature fragments) have to be reliably delivered to the LoRa NS. However, the ARQ scheme on the transport layer coupled to retransmissions (*i.e.,* 8 delivery attempts of every message) can significantly increase the performance of Multi-Packet transmissions.

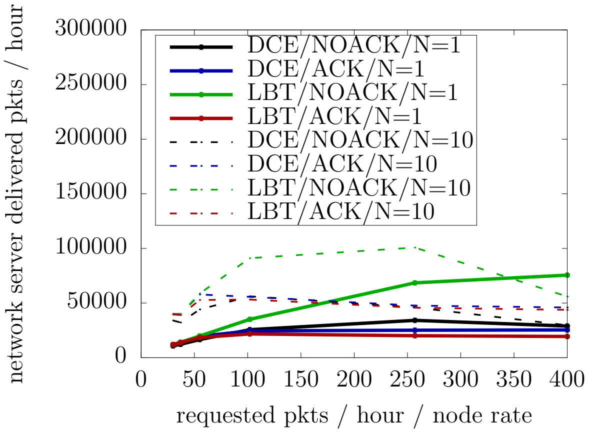

Fig. 7. Cumulative Throughput of the LoRaWAN Network, 1000 End-devices, 6 GWs

As expected, the LBT variant provided in CSMA-x [30] used in LoRaWAN significantly improves the network capacity (*cf.* Fig. 7). Throughputs of Multi-Packet transmission for $N = 10$ typically exceed the performance of Single Packet transactions by a factor of 2-2.5. This relation can be easily derived from the traffic pattern that has to be sent in both situations, i.e., data packet followed by two signature fragments in the Single Packet transaction scheme, against 10 data packets followed by two signature fragments in the $N = 10$ Multi-Packet situation.

Morever, the ACK mechanism significantly reduces throughput by a factor of two in the dense deployments, as in such a case, a GW has to shutdown listening to issue a downlink ACK packet.

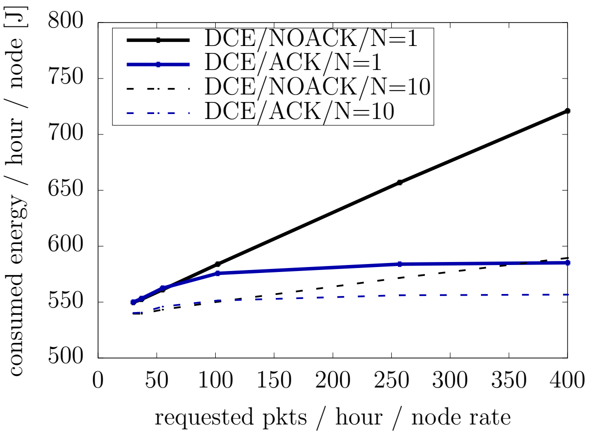

Fig. 8. Energy Consumption, 1000 Devices, 6 GWs.

Energy efficiency is considered as well (*cf.* Fig. 8). First, to reflect a real situation an Arduino[2] device equipped with a LoRa Dragino v1.4 shield[3] was measured in different states. The discovered parameters are summarized in Table II.

TABLE II
CHARACTERISTICS OF THE ARDUINO MEGA DEVICE.

Parameter	Value
Tension	5.1 V
Deep Sleep Current	0.029 A
Idle Current	0.087 A
CPU Computing Current	0.097 A
Idle Transmitter Current	0.010 A
Active RX Transmitter Current	0.016 A
Active TX Transmitter Current	0.095 A
Ed25519/SHA-512 signing	6.1 s

Second, the simulation was performed using the [22], [23] environment, who integrate their LoRaWAN module with the NS-3 Energy framework provided by [31].

Unfortunately, Arduino has an elevated Deep Sleep current, therefore, the results are not very significant. It is noted that the Multi-Packet scheme achieves the highest energy efficiency, however, the most dominant energy consumption comes from sleeping as in one hour the Arduino Mega devices consume 532 J. Moreover, the schemes were compared in the LoRa network saturation point, so the total number of transmitted messages (including data packets, signatures messages, etc.) is similar in all considered cases. However, the elimination of the heavy signing process of every data packet in Multi-Packet transactions provided much better performance in terms of energy efficiency for Multi-Packet transaction schemes.

VII. SUMMARY

Blockchain and IoT (BIoT) shed light on a broad range of applications which traditionally were developed in a centralized way without transparency provided towards end users.

[2] https://store.arduino.cc/mega-2560-r3
[3] https://wiki.dragino.com/index.php?title=Lora_Shield

Approaches employed to integrate IoT and BC lacked scalable transport mechanisms, which evaluate the throughput, energy efficiency, and reliability of the transmitted transactions. Please notice, however, the BC cost functions of different BCs supporting a given size and frequency of messages are left for future work. To achieve these goals, in this paper, the LoRaWAN network is being simulated and the achieved contributions are twofold.

First, to analyze the transmission behaviour of real-existing LoRaWAN devices, a data set covering TTN devices was processed. This implementation can be used to determine the geographical position of end devices in a definable area, which transmits in a regular fashion. Moreover, the developed applications provide the distribution of transmission periodicities among end-devices.

Second, an existing NS-3 LoRaWAN simulation module was enhanced by several components such that the simulation of blockchain-compliant LoRa networks became possible. At first, the code was extended to reach the goal of determining simulated networks' scored success rates as well as attained throughput in terms of successfully transmitted multi-packet transactions. Later, the simulation framework was equipped with LBT on end-devices, *i.e.,* to only transmit, if the channel was sensed clear beforehand. Moreover, the ACK/retransmission mechanism was introduced to improve data reliability. By running different simulation scenarios and scaling up simulated networks in terms of end device density as well as transmission frequency, the reused code adhering to DCE was compared against the LBT implementation. Comparing all scenarios, LBT introduced significantly improved success rates and throughput. Moreover, the throughput can be further increased by the Multi-Packet transaction schemes. Furthermore, the ACK mechanism trade the throughput achieved in the network for an increased transaction delivery ratio.

VIII. Acknowledgements

This paper was partially supported by (a) the University of Zürich (UZH), Switzerland and (b) the European Union Horizon 2020 Research and Innovation Program under grant agreement No. 830927, namely the Concordia project.

References

[1] A Technical Overview of LoRa and LoRaWAN. https://lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN101.pdf. Last visit: May 17, 2019.

[2] NS-3, A Discrete-Event Network Simulator. https://www.nsnam.org/. Last visit: May 17, 2019.

[3] OpenStreetMap. https://www.openstreetmap.org/copyright. Last visit: May 17, 2019.

[4] PROJ.4 library: Generic Coordinate Transformation Software. https://proj4.org/. Last visit: May 17, 2019.

[5] pyproj: Python Interface to PROJ.4 Library. https://pypi.org/project/pyproj/. Last visit: May 17, 2019.

[6] S2 Geometry Library. http://s2geometry.io/. Last visit: May 17, 2019.

[7] s2sphere: Python Implementation of a Part of the C++ S2 Geometry Library. https://s2sphere.readthedocs.io/en/latest/. Last visit: May 17, 2019.

[9] Spatial Reference: The World Geodetic System 1984. http://spatialreference.org/ref/epsg/wgs-84/. Last visit: May 17, 2019.

[8] Spatial Reference: The EPSG:21781 Projection (CH1903/LV03). http://spatialreference.org/ref/epsg/ch1903-lv03/. Last visit: May 17, 2019.

[10] The Things Network (TTN). https://www.thethingsnetwork.org/. Last visit: May 17, 2019.

[11] TTNMapper FAQ Page. http://ttnmapper.org/faq.php. Last visit: May 17, 2019.

[12] Norman Abramson. The Aloha System: Another Alternative for Computer Communications. *Proceedings of the November 17-19, 1970, Fall Joint Computer Conference*, AFIPS '70 (Fall), pp 281–285, Houston, Texas, 1970. ACM.

[13] F. Adelantado, X. Vilajosana, P. Tuset, B. Martinez, J. Melia-Segui, and T. Watteyne. Understanding the Limits of LoRaWAN. *IEEE Communications Magazine*, June 2017.

[14] A. Augustin, J. Yi, T. H. Clausen, and W. Mark Townsley. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. *Sensors*, 2016.

[15] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B. Yang. High-speed high-security signatures. *Journal of Cryptographic Engineering*, 2(2):77–89, September 2012.

[16] F. Van den Abeele, J. Haxhibeqiri, I. Moerman, and J. Hoebeke. Scalability Analysis of Large-Scale LoRaWAN Networks in NS-3 (Source Code on GitHub. https://github.com/imec-idlab/ns-3-dev-git/tree/lorawan. Last visit: May 17, 2019.

[17] F. Van den Abeele, J. Haxhibeqiri, I. Moerman, and J. Hoebeke. Scalability Analysis of Large-Scale LoRaWAN Networks in NS-3. *IEEE Internet of Things Journal*, 4(6):2186–2198, December. 2017.

[18] T. M. Fernández-Caramés and P. Fraga-Lamas. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*, 6:32979–33001, 2018.

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

[20] Maria Hernandez. Connectivity Now and Beyond; Exploring Cat-M1, NB-IoT, and LPWAN Connections. https://ubidots.com/blog/exploring-cat-m1-nb-iot-lpwan-connections/. Accessed: 2018-11-28.

[21] R. Khan, S. U. Khan, R. Zaheer, and S. Khan. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. *2012 10th International Conference on Frontiers of Information Technology*, pp 257–260, December 2012.

[22] D. Magrin, M. Centenaro, and L. Vangelista. Performance Evaluation of LoRa Networks in a Smart City Scenario. https://github.com/signetlabdei/lorawan. Last visit: May 17, 2019.

[23] D. Magrin, M. Centenaro, and L. Vangelista. Performance Evaluation of LoRa Networks in a Smart City Scenario. *2017 IEEE International Conference on Communications (ICC)*, pp 1–7, May 2017.

[24] A. Minaburo, A. Pelov, and L. Toutain. LP-WAN Gap Analysis. https://tools.ietf.org/html/draft-minaburo-lp-wan-gap-analysis-00, Feb. 2016. Accessed: 2018-11-28.

[25] É. Morin, M. Maman, R. Guizzetti, and A. Duda. Comparison of the Device Lifetime in Wireless Networks for the Internet of Things. *IEEE Access*, 5:7097–7114, 2017.

[26] U. Raza, P. Kulkarni, and M. Sooriyabandara. Low Power Wide Area Networks: An Overview. *IEEE Communications Surveys Tutorials*, 19(2):855–873, June 2017.

[27] B. Reynders, W. Meert, and S. Pollin. Range and Coexistence Analysis of Long Range Unlicensed Communication. *23rd International Conference on Telecommunications, ICT 2016, Thessaloniki, Greece, May 16-18, 2016*, pp 1–6, 2016.

[28] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent. LoRaWAN Specification v1.0.2. https://lora-alliance.org/resource-hub/lorawantm-specification-v102. Last visit: May 17, 2019.

[29] T. To and A. Duda. Simulation of LoRa in NS-3: Improving LoRa Performance with CSMA (Source Code on GitHub. https://github.com/drakkar-lig/lora-ns3-module. Last visit: May 17, 2019.

[30] T. To and A. Duda. Simulation of LoRa in NS-3: Improving LoRa Performance with CSMA. *2018 IEEE International Conference on Communications (ICC)*, pp 1–7, May 2018.

[31] H. Wu and R. Nabar, S.and Poovendran. An Energy Framework for the Network Simulator 3 (NS-3). *Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques*, SIMUTools '11, pp 222–230, Barcelona, Spain, 2011. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).