Secure Transmission of Immutable Data for Low-Power, Long-Range Wireless IoT Services

Andreas Baumgartner, Nada Akkari, Sudip Barua, Thomas Bauschert
Chair of Communication Networks, TU Chemnitz
Chemnitz, Germany
Email: [andreas.baumgartner | nada.akkari | sudip.barua | thomas.bauschert]@etit.tu-chemnitz.de

***Abstract*—In this work, we propose a network hierarchy to enable low-power IoT services applying the directed-acyclic graph (DAG) based Distributed Ledger Technology (DLT) IOTΛ Streams on top of the low-power wide-area network (LPWAN) protocol LoRaWAN. For LPWAN technologies, the challenges for applying distributed ledger application layer protocols are the small payload sizes and duty cycle regulations with open frequency spectrum protocols and the transport protocol limitations in massive-machine-type mobile communication protocol derivations (e.g. NB-IoT). For low-power embedded end devices, additional challenges may arise in terms of local computation limitations, which can be a limiting factor in performing necessary DL protocol-related functions at the device level (e.g. hashing, encryption) to maximize DL-related technology benefits end-to-end. In this paper, we show the concept of a scalable, feeless, low-power communication solution for reliable and secure data transmission and processing in sensor networks employing the DL technology IOTΛ based Streams protocol together with the LPWAN protocol LoRaWAN and demonstrate our design for the use case of a smart metering application.**

***Index Terms*—Internet of Things, DAG-based distributed ledger technology, LPWAN, LoRaWAN**

I. Introduction

Recent trends regarding IoT technology concern networks of distributed, self-managing, long-life battery-powered, and inexpensive devices while ensuring a high level of data security and integrity at the same time. For that reason, the family of LPWAN protocols has emerged as a cellular-like RAN technology optimized for IoT and massive Machine-Type Communication (mMTC) services in which low power consumption and low throughput are the intrinsic properties of the end-devices and their communication. Amongst already employed LPWAN protocols like NB-IOT [28], LTE-M or Sigfox [19], LoRaWAN is based upon the LoRa protocol for the wireless PHY layer, which provides long-range communications and robustness against interference by applying Chirp Spread Spectrum (CSS) modulation [7] for network operation in unlicensed frequency bands (433MHz ISM and 868MHz band). Next to the trends in machine-communication protocols, the advent of distributed ledger technologies enables the distribution and synchronization of ledgers for data and money in a secure, distributed, decentralized, and permissionless environment. Distributed ledger (DL) generally refers to the provision of consensus over a data set or system state amongst geographically distributed entities. Blockchain technology has primarily been applied as a key enabler for DL and has demonstrated proof-of-concept over the past years, with Bitcoin as a crypto-currency being the most prominent example [15]. The idea of blockchain technology is to synchronize a system that is asynchronous by nature via methods such as proof-of-work (PoW) or proof-of-stake (PoS) by which records can be filed securely on a ledger by miners and replicated by anyone. At its core, a blockchain-based DL is a linked list of record-storing blocks, where each block references the hash of the preceding block, making the stored data relatively tamper-proof. Directed acyclic graph (DAG) based distributed ledger protocols try to overcome the limitations of the initial blockchain technology (e.g. scalability, efficiency, storage, processing power) by allowing asynchronous branching and merging of the ledger's linked list. An example of a DAG-based distributed ledger protocol is the IOTΛ Tangle [1], [2] developed and introduced by the IOTΛ Foundation in 2017 and close to its 2nd protocol version IOTA 2.0. IOTΛ was designed to enable feeless micro-transactions and data integrity for machines to build a new permissionless machine economy, visioning an Internet of Things consisting of smart, autonomous and connected devices as economically independent entities inter-working over smart-contract or oracle-based rule chains. In this work, we propose a protocol stack for low-power IoT applications based on IOTΛ's DL technology Streams (as an application layer) on top of the LPWAN protocol LoRaWAN to realize a secure IoT communication network infrastructure for low-power long-range wireless IoT services.

The concept is part of the SUSEE project, which is focused on the conceptual design of a DL-based platform for the energy grid and electricity market.
The proposed concept comprises the following innovations:

- Utilization of the DAG-based DLT protocol IOTA Streams on low-power embedded hardware.
- Adaptation of transport layer and control plane functionalities to enable reliable data exchange for packet streams over LoRaWAN, applying IOTA streams.
- Minimization of overall wireless channel occupation with the help of local desynchronization algorithms.
- Implementation of a transport layer protocol comprising the innovations and control plane functionalities and to complete a low-power protocol hierarchy for secure IoT services.

The rest of this paper is organized as follows: In Chapter

2, we present the technological background of the proposed protocol hierarchy. In Chapter 3 the overall concept together with the necessary protocol hierarchy for Efficient LoRaWAN Channel Access and Packet Streaming over LoRaWAN is presented. Additionally, the setup for a DVSGO-compliant (i.e. German version of the GDPR) smart meter application is shown. Chapter 4 comprises a discussion of the conceptual approach. Finally, in Chapter 5, a conclusion of this work is provided.

II. Motivation and Technology Overview

A. Low Power Wide Area mMTC

For Internet of Things services, in the context of next-generation mobile communication 5G, the application classes "Ultra-Reliable Low-Latency Communication" (URLLC) and "massive Machine-Type Communication" (mMTC) are specified. URLLC refers to IoT services that require a high level of availability, i.e. 99.999% success rate for a 32 Byte packet transmission within 1ms [29] - not the overall network availability, without focusing on power efficiency for long-term, potentially energy self-sufficient device operation. For this purpose, mMTC devices comprising low bandwidth and latency requirements thereby facilitating a large number of simultaneous connections with low power consumption transmission are specified [30]. In 3GPP Release 17, the first standardization for mMTC end device communication called "NR-light" was completed in March 2022 with the first chipsets expected to be available at the end of 2024. For the technological readiness level at the time of the project start, only NB-IoT, LTE-M in licensed, and LoRaWAN and Sigfox in unlicensed frequency spectrum were available for deploying mMTC services.
LoRaWAN is an open communication network protocol based on the LoRa technology [7], [20] and is standardized by the LoRa Alliance, which is an open, non-profit association of members [8]. LoRa(WAN) belongs to the family of LPWAN protocols, which are intended for large-scale networks comprising low power and low throughput end devices with asynchronous bi-directional communication patterns (see also Low Throughput Networks [9]). While LoRa defines the physical layer enabling long-range communication in an unlicensed spectrum with very low power consumption by using Chirp Spread Spectrum (CSS) modulation (with different spreading factors), LoRaWAN defines the data link layer protocol. Some key features of the LoRaWAN/LoRa technology are:

- Simple, yet scalable core network architecture consisting of LoRaWAN network and application servers. Both of the components are available as open-source software and can even run on small, low-power embedded end devices [14]. The networks can be operated privately worldwide due to the license-free spectrum range LoRa was designed for.
- Adaptable payload sizes from 51 – 250 Bytes (depending on optional header configuration [5]) using a channel bandwidth of 125kHz. Additional 250kHz bandwidth is available, which increases the maximum bitrate to 11000 bits/seconds at a maximum payload size of 222 Bytes. Compared to the NB-IoT LPWAN protocol [28], which offers up to 1600 Bytes payload, this seems to be small, but significant compared to the 12 Byte maximum payload size in the Sigfox LPWAN technology [7].
- No device-to-base station allocation in a LoRaWAN network. Packets are received by every base station in reach.This capability is intended to allow larger-scale machine communication compared to classical mobile communication systems. In real LoRaWAN network deployments, a packet is received on average by 6 up to 28 different base stations [24].
- A LoRaWAN network is deployed in a star-type topology with the gateways (i.e. base stations) acting as transparent bridges.
- 2 level of 128 Bit Key AES ECB Ciphering as standard LoRaWAN security, enabling the separation of network infrastructure and service provider business models.

For a detailed overview of the LoRaWAN/LoRa technology features refer to [7].
Additionally, for LPWAN protocols operating in the unlicensed frequency spectrum, an end device needs to retain within duty cycle regulations (i.e. maximum allowed channel occupation time, in EU 868 MHz ISM radio band typically 0.1 %, 1.0 %, 10.0 %) for its communication, which sets an upper limit for the maximum of communicable data volume over the air depending on the spreading factor (i.e. transmission channel conditions). In principle, the number of packets is subject to the data volume and type to be transmitted. This restriction is particularly tighter for LoRaWAN due to the narrow bandwidth and low-duty-cycle regulations. If the amount of data exceeds the maximum payload size of a LoRaWAN packet a sensor has to fragment the data into several packets and send them sequentially.

In this work, the LPWAN protocol LoRaWAN is employed for communication as it provides a good power consumption to communication robustness at minimum operational costs at the limit of technical feasibility.

B. DAG-based networking for secure exchange of immutable data

The vision of a machine economy comprising smart, autonomous peers, inter-working over a network employing smart contract-based rule or service chains and oracle procedures implies a high level of data privacy, integrity and authenticity. If additionally full-autonomous economic processes are involved, consensus over data from all distributed peers as well as data privacy and immutability is required. For that reason, distributed ledger technology is seen as a key enabler for IoT technology with directed-acyclic graph-based DL as a promising research area to enhance scalability and performance over traditional blockchains [30].

As an example of a DAG-based DLT, IOTΛ is developed by the IOTΛ Foundation since 2016 and is one of the candidate

protocols for the European Commission's Blockchain Pre-Commercial Procurement [3]. IOTΛ Streams is a second layer protocol to enable navigating secure data with a data access privilege management on top of the DLT. It can be seen as an organizational tool for structuring data and controlled data sharing access (within a defined set of publishers and subscribers) [23].

LPWAN communication protocols, like LoRaWAN or NB-IoT, on the other hand, are designed to provide long-range, low-power communication for IoT devices with constrained processing resources. Therefore, ensuring secure communication over LPWAN poses several requirements and challenges on cryptographic and security-related protocols in terms of efficient encryption and authentication mechanisms while minimizing resource consumption. Compared to other State-of-the-Art cryptographic protocols that can be adapted to fit LPWAN protocol requirements like LoRaWAN, e.g. Transport Layer Security (TLS) in the classical TCP/IP or Datagram Transport Layer Security (DTLS) for UDP/IP connections, the data volume of a Stream transaction object in a typical low-power IoT application is low, e.g. ∼250 Byte for the demo smart metering application, refer to III-C. A full TLS handshake, which ranges between 3 kByte and 6 kByte (depending on the cipher suite used), has been demonstrated to produce bottlenecks in large-scale LPWAN network deployments with license-free spectrum in the downlink direction, because of the resource-intensive nature of the protocol's hand-shaking procedure and duty cycle regulations [25]. In comparison: IOTΛ Streams make a key exchange and therefore heavier downlink data transmission traffic only if the owner, tenant, or operator of the metering point or the service provider is changing and the respective access to the sensor data over the DLT has to be reorganized.
With the help of on-hand DL and LPWAN technology, in the next chapter, we explain the concept of a low-power, fee- and permissionless network architecture.

III. Concept

A. System Architecture

To exploit all of the technical benefits from DLT in terms of trust, reliability, ownership, security and privacy, a wireless connected sensor in the field must be capable of processing distributed ledger protocol functions directly, i.e. executing required algorithms (ciphering, hashing and general data processing), to create a DL-compatible transaction object containing all relevant device data. This transaction object in turn can be transmitted using LPWAN technology.

If the communication protocol or the communication channel allows only for a limited packet size or transmission rate (e.g. due to duty-cycle limitations in the unlicensed frequency spectrum), the transaction object needs to be fragmented and sent over the air as a sequence of packets. For the LPWAN protocol LoRaWAN the wireless transmission might apply different spreading factors (offered by the LoRa PHY) depending on the transmission channel and the device mobility. In Figure 1, the architecture of the proposed system design

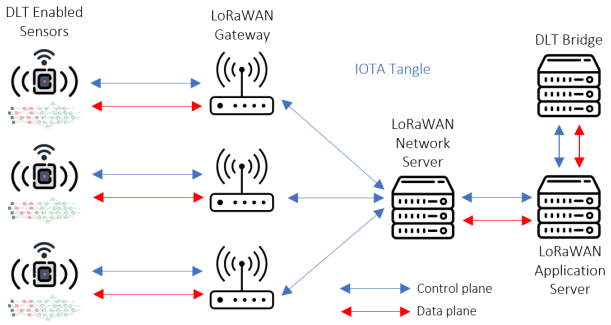

Fig. 1. System concept

is outlined: LoRaWAN packets, containing IOTΛ encoded data, are received from gateways and forwarded to the network server, which handles device registration and packet de-duplication. After the application-specific content is received by the application server, the IOTΛ Streams transaction objects can be reassembled and queued to be attached to the DLT. For that purpose we introduce an additional network element, the DLT bridge, acting as a stateful intermediate node between the end devices and the distributed ledger. For setting up an IoT service that applies a distributed ledger technology, the sensor requires an initialization phase to set up the necessary device keys. In the case of IOTΛ Streams, the necessary Streams channel has to be created, and the subscription and publication rights (e.g. customers, service provider, IoT service provider) have to be granted access to the respective entities and tenants. Every security and identity-related information of a peer within the IOTΛ network is directly derived from the seed, the most security-relevant information for an IOTΛ peer. In our system architecture and implementation, the sensor platform is the only peer in the system architecture knowing the seed, securely stored on the embedded hardware, for deriving all IOTΛ and Streams-related information, which guarantees a high level of security (i.e. data integrity). Private keys are derived from the seed (with a key index offset). From that private key, the sensor can then generate an address. If the sensor wants to send an IOTΛ Streams message, it initializes a transaction object using the generated addresses from the seed and the generated information for the Streams channel publication, which has been set up at the initialization phase of the sensor.
In our concept, a WiFi connection is provisioned for the initial system setup, due to bandwidth limitations of LoRaWAN. After the initialization phase, the sensor can exploit the advantages of the IOTΛ Streams protocol as the only publisher in his own Streams channel over the LPWAN protocol LoRaWAN, and adapt Streams and plain LoRaWAN data transmission according to the requirement of the specific IoT use case or the IoT service/network provider.

B. Efficient LoRaWAN Channel Access and Packet Streaming

After the initialization phase, all device communication is handled by exploiting the LoRaWAN communication link.

LPWAN protocols are designed to minimize overall power consumption for device communication, keeping necessary algorithmic complexity, synchronization and hand-shaking procedures to a minimum level. Especially for LPWAN protocols operating in the unlicensed frequency spectrum range, the channel access mechanism is similar to that of the pure ALOHA protocol [18], in which a transmitting device is oblivious to the state of the shared communication channel. If dynamic changes in network conditions, such as changing traffic loads, changing user requirements or a dynamic number of communicating network nodes appear, flexible and adaptive allocation algorithms are required to avoid overall network performance degradation due to suboptimal resource utilization (i.e. effects like decreased service availability, increased number of retransmission and shorter battery-powered lifetime expectations for devices).

In the context of LPWAN protocols and especially considering LoRaWAN as an example communication protocol, several contributions have been published to enhance overall system performance by adapting the ALOHA-like channel access mechanism of many LPWAN protocols [16], [21], [22]. Additionally, when applying IOTΛ Streams on top of LoRaWAN for wireless connectivity of an IoT application, depending on the required data volume for the service, the transaction object may need to be split and send as a sequence of LoRaWAN packets. In that case, single packet retransmission and the handling of sequences of packets can be handled by exploiting LoRaWAN acknowledged transmission mode (in all LoRaWAN device classes), predefined FPort ranges, and a minimal control plane functionality overhead by employing a downlink-side command structure and a payload-header for the single LoRaWAN packets (i.e. version, revision, checksum). With the help of the MAC layer and Control-plane extension, LoRaWAN can be used to interwork with DLT-based networking protocols like IOTΛ (Streams) and its successor IOTΛ 2.0.

C. Smart Metering Application

To study the performance of the proposed concept, a smart metering hardware sensor platform was designed to pull energy metering relevant data from an IM's ("intelligente Messsysteme") or Smart Meters and transmit the data using IOTΛ over LoRaWAN. A challenge facing the widespread adoption of smart meters is data security. In Germany, wireless smart meters have to meet stringent requirements in privacy, data integrity, and interoperability, as regulated by the DS-GVO. To comply with this specific regulation, any system that processes personal data must guarantee the confidentiality of the collected data and usage of data only if necessary to fulfill the service. Additionally, if user metering data is used for fully automated billing processes, smart meters need to comply with the Measuring Point Operation Act (Messstellenbetriebsgesetz) and follow the guidelines of the Federal Office for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik). It must also guarantee that the end-user has explicitly consented to data collection and that this consent can be revoked at any time. As most of the commercially available SoC microprocessors for LPWAN communication do not have enough computing power for processing distributed ledger-based application layer protocols, an additional application processor (ESP32 C3 mini) is included in the demonstrator hardware. The processor is powerful enough to process the IOTΛ Streams-related libraries, i.e. initialization, execution of hashing and ciphering-related functions necessary for the attachment to the DLT and the application and control plane-related functions. The software libraries to enable the second layer DLT protocol $IOT\Lambda$ Streams to work on a small, low-power, inexpensive embedded system were written in RUST and provided by the IOTΛ foundation. To achieve stable Streams over LoRaWAN communication from the sensor side, the project partners developed additional software libraries in C for the protocol extensions from III-B. These libraries handle LoRaWAN communication as a socket on the application processor, either in combination with the communication SoC Chip (Ascip) or directly at the LoRaWAN SoC chip, which acts as a pre-baseband processor. Additional software has been implemented at the level of the communication chip to get timestamps relevant to sensor measurements on the application and on the communication chip to meet regulatory requirements and policies of the acquired data defined by the government and company/customers. For utility companies or energy grid providers, a typical target time interval for smart meter readings is 15 minutes. In the case of the lowest spreading factors 7 and 8, two LoRaWAN packets are required to transmit the relevant smart meter information from a sensor, encoded with IOTΛ Streams, over the air. These spreading factors reflect the most typical/relevant channel conditions for well-developed LoRaWAN networks in smart city scenarios [24], if the sensors are operated with the LoRaWAN Adaptive Data Rate (ADR) feature enabled. This enables fast transmission of all billing-relevant information together with a unique and immutable sensor identity, in the context of LPWAN or Low Throughput Networks [9] characteristics. Even for the highest spreading factor 12, which is characteristic of very challenging transmission channels or long-range non-sight connection types, the transaction object can be transmitted by exploiting 7 LoRaWAN packets.

IV. Discussion

This concept makes IOTΛ streams-based data transmission compatible with all modulation schemes and spreading factors that are available for a LoRaWAN-certified chipset (i.e. LoRa, FSK). As the sensor data was ciphered by the sensor itself, even a compromised middleware server cannot manipulate or change the stream of encoded information transmitted from the sensor. Even changing the level of publication or access to the sensor's data can only hardly be exploited. These statements are also true for the case of a corrupted LoRaWAN network server or the whole network. The worst-case scenario of a corrupted network or middleware server would be the non-attachment state of the data, that the sensor sends to the network. This artifact can be monitored and registered by both

the distributed ledger and the IoT communication network management system, and respective counter-measures can be taken, including the change of all Streams-related channel publication and subscription rights, and re-generation of all IOTΛ related keys on Downlink command or using local wireless communication.

Applying IOTΛ Streams as a 2nd layer DL protocol for an IoT application at the sensor side can add a new level of data security as well as integrity and immutability to an IoT application or service (even including billing relevant information). Besides IOTΛ Streams parts of the implementation, results and tests within this work can be used to add further second layer protocols over IOTΛ to incorporate service automation like a smart contract or to further increase system security and performance. Moreover, footprint analysis can be done leveraging outsourced computation protocols or permanodes as storage of relevant data over longer periods without an actual monetary transaction. The ideas presented in this paper may also be applied to other LPWAN standards, depending on the system parameters and payload sizes as well as other distributed ledger or non-distributed ledger-based protocols (MQTT-SN) that meet the architectural requirements and options for building IoT systems over LPWAN networks using small embedded systems as hardware platforms.

Our concept can be used as a part of a larger IoT LoRaWAN network, comprising a much larger number of IoT sensors and data flows, which are not related to the DL-enabled smart metering application architecture that we present in this paper. LoRaWAN networks show good scalability and low packet loss if they are operated with proper settings [17], [24]: Trials in dense urban environments showed that LoRaWAN networks can deliver high packet transmission success rates (reaching from 96 % up to 99.9999 % in [11]), even in unlicensed spectrum and only with ALOHA channel access policies. Problems may arise if it is required to send a sequence of packets when the size of transmission data exceeds the maximum packet size. In such situations packet losses are inevitable due to the ALOHA-like channel access mechanism if the network infrastructure is not well expanded. Besides this known limitation, the studies in [17] show that not all channels are used evenly in the LoRaWAN networks, which increases packet loss as well. For battery-powered sensors with acknowledged transmission mode, every re-transmit attempt has a negative impact on the battery lifetime.

V. Conclusion and future work

For some researchers, modern DL technology is seen as one of the key innovations enabling secure IoT services, but the technology is still considered to be in its infancy. This work is intended to demonstrate the capabilities achievable by combining feeless and open state-of-the-art LPWAN in unlicensed frequency spectrum together with DAG-based DLT for embedded sensor platforms with the help of a DSGVO-compatible smart metering application. Our work demonstrates the usage of DLT for machine ecosystems in the context of LPWAN communication and shows how far the technologies have already grown together in terms of adaptability in the context of secure low-power IoT services and networks. Unfortunately, the focus of DLT research shifted from IoT-related topics, where this technology can be a key enabler, to DeFi interoperability and 2nd layer protocol issues to reduce the number of relevant DLT protocols from a techno-economical perspective. The primary issue for large-scale IoT applications applying DLT is still the low scalability and network throughput, which DAG-DLT tries to solve. Additionally, we further want to enhance the system's performance by adapting further desynchronization algorithms between the DL application layer and the MAC layer provided by LoRaWAN as mentioned in chapter III-B and extend the protocol hierarchy for moveable objects. Our concept is field tested for practical experience starting at Q2/2024 and extended for compatibility to IOTΛ 2.0.

Acknowledgment

This work was funded in the context of the SUSEE project by the Applied Non-Nuclear Research Funding in the 7th Energy Research Program "Innovations for the Energy Transition" of Germany's Federal Ministry for Economy and Energy (BMWK, ID 03EI6047A). We thank the IOTΛ foundation, TIP GmbH, peerOS GmbH, and mCloud Systems GmbH for the many contributions to the concept as well as Tobias Tuchscherer, Tuan Khai Nguyen from TU Chemnitz.

References

[1] S. Popov, "The Tangle", available on: https://www.iota.org/
[2] https://blog.iota.org/iota-eu-blockchain-pcp/, 2023.
[3] https://digital-strategy.ec.europa.eu/en/news/european-blockchain-pre-commercial-procurement, 2023.
[4] Javascript Version: https://github.com/iotaledger/iota.lib.js
[5] "LoRaWAN specifications V1.1", https://lora-alliance.org/lorawan-for-developers/, 2023.
[6] LoRa Alliance, "What is LoRaWAN? A technical overview of LoRa® and LoRaWAN™", https://www.lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf, 2015.
[7] https://www.semtech.com/technology/lora
[8] https://www.lora-alliance.org/
[9] European Telecommunications Standards Institute, "Low Throughput Networks", https://www.etsi.org/technologies-clusters/technologies/low-throughput-networks, 2014.
[10] LoRaWAN regional parameters V1.0.2 https://lora-alliance.org/resourcehub/rp2-102-lorawan-regional-parameters/, 2023.
[11] R. Gilson, M. Grudsky "LoRaWAN Capacity Trial in dense urban environment", https://info.semtech.com/hubfs/machineQLoRaWANCapacityTrial-2.pdf?hsLang=en-us, 2023.
[12] K. Mekki, E. Baji, F. Chaxel, F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment", https://doi.org/10.1016/j.icte.2017.12.005, 2018.
[13] M. Centenaro, L. Vangelista, A. Zanella, M. Zorzi, "Long-Range Communications in unlicensed band: The rising stars in the IoT and smart city scenarios", IEEE Wireless Communications, October 2016.
[14] https://www.chirpstack.io/
[15] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", available: https://bitcoin.org/bitcoin.pdf.
[16] K. Spathi, A. Valkanis, G. BeletsIoTi, G. Papadimitriou and P. Nicopolitidis, "Performance Evaluation of Slotted ALOHA based IoT Networks under Asymmetric Traffic," 2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), Sharjah, United Arab Emirates, 2020, pp. 1-5, doi: 10.1109/CCCI49893.2020.9256406.

[17] N. Blenn, F. Kuipers: “LoRaWAN in the Wild: Measurements from The Things Network”, arXiv: 1706.03086v1, 2017.
[18] N. Abramson, “The ALOHA System - Another Alternative for Computer Communications”, AFIDS Conference Proceedings, Band 37. AFIPS Press, 1970, p. 281–285.
[19] Sigfox: https://www.sigfox.com/
[20] http://www.3glteinfo.com/lora/lora-architecture/
[21] M. Baddula, B. Ray and M. Chowdhury, ”Performance Evaluation of Aloha and CSMA for LoRaWAN Network,” 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 2020, pp. 1-6, doi: 10.1109/CSDE50874.2020.9411539.
[22] Degesys, Julius, Ian Rose, Ankit Patel, and Radhika Nagpal, ”DESYNC: Self-Organizing Desynchronization and TDMA on Wireless Sensor Networks”, Harvard Computer Science Group Technical Report TR-18-06, 2006.
[23] https://www.iota.org/solutions/streams, 23-05-16.
[24] T. Horstmann, M. Rademacher, M. Roobi, S. Weckmann, ”Evaluation of LoRa in a Real-World Smart City: Selected Insights and Findings”, ITG-Fb. 311: Mobilkommunikation – Technologien und Anwendungen, Vorträge der 27. VDE ITG-Fachtagung p. 91 - 96, 2023.
[25] M. Rademacher, H. Linka, J. Konad, T. Horstmann, ”Bounds for the Scalability of TLS over LoRaWAN”, Mobile Communication - Technoloies and Applications; 26th ITG-Symposium, pp. 1 - 6.
[26] https://mcloud-systems.com/, 2024.
[27] https://www.peeros.de/, 2024.
[28] R. Rarasup, N. Mangalvedhe, Y. Zhang, M. Robert, J.-P. K., ”Overview of Narrowband IoT in LTE Release 13”, IEEE Conference on Standards for Communications and Networking (CSCN), 2018.
[29] ITU-R Report M.2411-0 (11/2017), https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2411-2017-PDF-E.pdf, 28.07.2022
[30] ITU, Draft Recommendation: Requirements of IMT-2020 from network perspective, Dec. 2016.
[31] Akhtar, M.M.; Rizvi, D.R.; Ahad, M.A.; Kanhere, S.S.; Amjad, M.; Coviello, G. Efficient Data Communication Using DLT and IOTA-Enabled Internet of Things for a Future M2M Economy. Sensors 2021, 21, 4354. https://doi.org/10.3390/s21134354
[32] Askhedkar, A., & Chaudhari, B. (2023). Multi-armed Bandit Algorithm Policy for Lora Network Performance Enhancement. Journal of Sensor and Actuator Networks, 12(3), 38. https://doi.org/10.3390/jsan12030038
[33] Aihara, N., Adachi, K., Takyu, O., Ohta, M., & Fujii, T. (2019). Q-Learning Aided Resource Allocation and environment recognition in Lorawan with CSMA/Ca. IEEE Access, 7, 152126–152137. https://doi.org/10.1109/access.2019.2948111