Reliable Data Transmission using Low Power Wide Area Networks (LPWAN) for Agricultural Applications

Franz Kuntke
kuntke@peasec.tu-darmstadt.de
Technical University of Darmstadt
Darmstadt, Germany

Marcel Sinn
sinnmarcel88@gmail.com
Technical University of Darmstadt
Darmstadt, Germany

Christian Reuter
reuter@peasec.tu-darmstadt.de
Technical University of Darmstadt
Darmstadt, Germany

ABSTRACT

Reliable IT-based communication in agriculture is becoming increasingly important for regular operations. For example, if a farmer is in the field during a network outage, such as a failure of the mobile network, an alternative communication channel is needed to continue to connect to IT components and required data. With increasing digitalization, Low Power Wide Area Network (LPWAN) technologies are being used more and more frequently, e.g. for sensor networks. The LPWAN technologies offer a high range and can be used autonomously for the most part, but do not allow classic TCP/IP communication. In this work, a popular LPWAN technology, namely LoRaWAN, is experimentally supplemented by AX.25 on OSI layer 2 (Data Link Layer) to allow end devices TCP/IP-based communication over long distances. The evaluation shows that classic low-bandwidth applications are thus functional and can enable reliable, crisis-capable data transmission.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

KEYWORDS

redundant data transmission, reliable wireless channel, LPWAN, LoRa, agricultural application

ACM Reference Format:
Franz Kuntke, Marcel Sinn, and Christian Reuter. 2021. Reliable Data Transmission using Low Power Wide Area Networks (LPWAN) for Agricultural Applications. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3465481.3469191

1 INTRODUCTION, BACKGROUND AND RESEARCH QUESTION

Digitalization is now more than ever permeating all areas of the life of modern people. Smart Home is a familiar concept for everyone, ranging from the smart coffee machine to the smart door lock. But also industry sectors, including critical infrastructures, like agriculture, become more complex and interconnected through digitalization [21] . In order to make agricultural systems intelligent, techniques from the fields of 'machine learning' [24] and 'big data' are also used to further support farmers and autonomous systems [42]. The objective of smart farming is to emancipate from stationary control and monitoring systems of a farm. Control interfaces are now available on common end devices such as smartphones [37] and tablets. This makes it possible to perform everyday tasks remotely. Also common to almost all processes and techniques, regardless of the type of application, is that they require a communication channel for the purpose of signal or data transmission. For regular operations in agriculture, communication with other actors is necessary, which, as described, increasingly takes place via digital channels [23]. A product research of different large manufacturers has shown that the available (relevant) possibilities are currently the following: mobile radio, LAN, WLAN, Bluetooth, satellite, proprietary radio solutions, USB, LoRaWAN, and NB-IoT.

'Narrowband Internet of Things (NB-IoT)' and 'Long Range Wide Area Network (LoRaWAN)' belong to the so-called 'Low Power Wide Area Networks (LPWAN)' [14]. LPWAN are different radio technologies that aim to work using as little energy and as cost-efficient as possible while at the same time trying to maximize the radio range. They are often used in the IoT sector [3], where it is important to connect the highest possible number of devices. The aforementioned characteristics also predestine LPWANs for agriculture, where large arable land, livestock pastures, or stables exist. This is particularly evident in countries with huge farming areas such as China, the USA, or Australia.

Despite all the benefits for humans, animals, and the environment, smart farming also brings challenges [4]. Given the current dependence of agriculture on digitalization, an outage of technology can potentially cause great damage. For example, the barn climate has a direct influence on the health of the animals [38], so an outage of the air-conditioning system is considered critical. The 'Federal Ministry of the Interior, Germany (BMI)' in 2016 issued an ordinance [7], which lists, among others, the sectors energy, water, information technology, and telecommunications as critical infrastructures. Of particular note is the inclusion of the food sector. This encompasses agricultural companies, which, according to the ordinance, are particularly worthy of protection. To an increasing degree, the focus it hence put on implementing interconnectedness along the food supply chain in a crisis-proof manner [28]. This is reflected in current research approaches [35], which support the idea of making smart farming resilient.

However, crises do not have to have the scale of a war or a nationwide environmental disaster to cause damage to agriculture and industry. Scenarios such as the outage (of parts) of the Internet or local emergencies also have significant potential to cause major

---

ARES 2021, August 17–20, 2021, Vienna, Austria

ACM ISBN 978-1-4503-9051-4/21/08…$15.00
https://doi.org/10.1145/3465481.3469191

damage. After Egypt was cut off from the rest of the Internet for five days in 2011, the cost to Egypt's economy was estimated to be at least $90 million [20]. For countries heavily dependent on the internet, the authors estimate the damage at $23.6 million per 10 million inhabitants. Because of its enormous impact, research is also engaged in illuminating the scenario of internet outages [1]. Also, sector-specific phenomena like 'Agro-Terrorism' [36] pose a potential threat in the field.

The research question that arises and which is to be answered in the context of this work reads as follows: *In times of increasing digitalization in agriculture, how can reliable data transmission to minimize or partly avoid the effects of local crises (outages of the internet/mobile network, radio gaps) with regard to operational safety-relevant processes, be realized?*

In this work, a data link & network layer is to be evaluated for a selected physical layer. It is important that integration into the existing IT landscape with minimum effort, high interoperability, and compatibility is possible. For this purpose, the existing protocols for the physical layer are examined. Taking into account current research, trends, and the increasing demands and framework conditions developed, our own concept is presented.

2 RELATED WORK AND COMPARISONS OF LPWAN TECHNOLOGIES

LPWAN technologies are closely linked to the IoT, which is also gaining importance in agriculture. Raza et al. [34] give a comprehensive introduction to the topic of LPWAN technologies in general. Chaudhary et al. [8] analyze LPWAN technologies specifically in the IoT context. Here, they consider NB-IoT, RPMA, SigFox as well as LoRaWAN. Among other things, the different approaches, advantages and disadvantages, bandwidth, range, as well as the type of applications for which the respective technology is best suited are highlighted. Civelek [10] also deal with LPWAN technologies but in the agricultural context. The author describes IoT as particularly useful for agriculture and highlights the increasing importance of wireless technologies. He also attributes to LPWAN technologies the increasingly important characteristics of security, reliability, low installation, and operating costs. In addition to mobile communication, WiMAX and LoRaWAN with long-range, WiFi, Bluetooth, and RFID with short-range are also compared with regard to agricultural applications. They recommend LoRaWAN for large ranges and Bluetooth 4.0 for short ranges. Finally, the author develops an application example and uses LoRaWAN as a transmission technology for a tractor data acquisition system. An idea for using LoRa-based peer-to-peer communication in emergency scenarios is found in the work of Höchst et al. [17]. They propose a low-cost companion device, consisting of a LoRa transceiver including an onboard Bluetooth chip that is connected via Bluetooth to a self-developed messaging app on a smartphone, which allows for infrastructureless text communication. A practical evaluation shows that their approach could allow peer-to-peer chats with a communication distance up to 2.89 km in an urban environment with low-cost LoRa hardware. Xu et al. [43] design and implement a LPWAN network based on the LR(Low Rate) WPAN standard 'IEEE 802.15.4' for monitoring critical infrastructure and facilities in cities. A long range is cited as a critical requirement for such a network. In a test bed, it could be shown that the system works well within a radius of about 3 km. A similar paper to the aforementioned article using LPWAN technology but set in the context of agriculture and critical infrastructure was not found at the time of the search. This work intends to take this circumstance into account. In the following, a comparison of different LPWAN physical layers is conducted in order to evaluate the most suitable physical layer, taking into account the context and previously defined requirements.

Table 1: Overview - LPWAN Technologies and Sources

LPWAN Technology	*Sources*
Sigfox	[18], [6], [26], [27], [25], [19], [39], [41], [16]
NB-IoT	[18] [26], [27], [25], [39], [41], [16]
LoRa(WAN)	[18], [6], [26], [27], [25], [19], [39], [41], [16]
RPMA	[18] [6], [25], [19], [41], [16]
D7AP	[6], [25], [41]
*Weightless-**	[6], [25], [19], [41], [16]
MIOTY	[41], [16]
NB-Fi	[25], [41], [16]

Due to the ability to bridge long distances with low energy expenditure, there is now a multitude of different LPWAN technologies, so it is first necessary to identify them and thus create an overview. Therefore, various papers, journals, and market analyses were considered, and the previously mentioned product analysis was used to provide the broadest possible overview of technologies from research and industry. Table 1 lists the identified LPWAN technologies and their researched sources. Eight relevant LPWAN technologies could be identified, with Sigfox, NB-IoT, and LoRa(WAN) being the most popular, more specifically, the most widespread ones. The presented technologies and physical layer, as well as the characteristics relevant for this work, are summarized in the following Tables 2 and 3. The feasible maximum values are always referenced. Since LPWANs by definition have a low energy consumption, which may vary depending on the scenario and the higher layers used, this characteristic is not included in the tables.

One of the most important requirements for a communication channel during a local crisis is provider-independent network operation [15]. This eliminates the technologies SigFox and NB-IoT as potential candidates in the selection since they can only be operated via an 'Internet Service Provider (ISP)'. As explained in the beginning, agricultural areas are very large, which is why the range plays an essential role. The Weightless-N, Weightless-P, and D7AP technologies are ruled out because their range is - comparatively - too short. Moreover, Weightless-N only intends an uplink so that messages can only be sent but never received. Even though LPWANs do not achieve high data rates due to their technical characteristics, it is still desirable to achieve the highest possible data throughput. From this point of view, the MIOTY and NB-Fi technologies are eliminated because, at 407 bps and 100 bps, respectively, they do not reach the kbps mark as the rest of the technologies.

It is now to decide between the last three technologies, LoRa, RPMA, and Weightless-W. Of these technologies, LoRa has the highest range and Weightless-W the lowest. Weightless-W, on the other hand, allows the highest data rates and RPMA the lowest. One of the issues with Weightless-W is the utilization of 'TV white spaces'.

Table 2: Comparison - LPWAN Technologies - Part 1/2

	SigFox	*NB-IoT*	*LoRa(WAN)*	*RPMA*	*D7AP*
Technology	UNB	LTE	WB/SS	SS	2-GFSK
Band	ISM	LTE/GSM	ISM	ISM	ISM
Network Operation	ISP	ISP	ISP/Private	ISP/Private	Private
Data Rate	Up: 100 bps Down: 600 bps	250 kbps	50 kbps	Up: 78 kbps Down: 19,5 kbps	166 kbps
Range	50 km	10 km	30 km	15 km	2 km
Link Budget	159 dB	164 dB	154 dB	177 dB	140 dB

Table 3: Comparison - LPWAN Technologies - Part 2/2

	Weightless-N	*Weightless-P*	*Weightless-W*	*MIOTY*	*NB-Fi*
Technology	UNB/DBPSK	NB/GMSK+OQPSK	WS/Variabel	UNB/TS	NB/DBSK
Band	ISM	ISM	WS	ISM	ISM
Network Operation	ISP/Private	ISP/Private	ISP/Private	Private	ISP / Private
Data Rate	Up: 100 bps Down: n/a	100 kbps	1 kbps - 10 Mbps	407 bps	100 bps
Range	5 km	2 km	10 km	15 km	50 km
Link Budget	n/a	147 dB	Variabel	154 dB	176 dB

These frequencies are not available or approved in all countries. In addition, distribution and hardware availability seems to be very limited. No freely available hardware components or information about networks in use could be found at the time of the research. Due to this and its relatively short range compared to the remaining technologies, Weightless-W is eliminated as a candidate.

In direct comparison, LoRa has twice the range of RPMA. The data rates are, depending on the higher layer used, higher with LoRa (Symphony Link). Only in comparison with LoRaWAN (approx. 50 kbps), RPMA has an advantage in the uplink (78 kbps), but only a very low downlink (19.5 kbps). One advantage of RPMA is the use of the free 2.4 GHz band, where there is no duty cycle. In [33], the future safety of LoRa is predicted to be five times better than RPMA. This is also reflected in a product analysis, which has already identified LoRaWAN-capable products. The fact that there are two other productive LoRa-based protocols in addition to LoRaWAN, namely Symphony Link and DASH7, underscores this assessment. In the conference paper of Vangelista et al. [40], LoRa is described as the most promising technology in the field of ‘wide-area IoT’. Another advantage is the broad hardware availability from low-cost DevKits to complete gateways. Based on the arguments presented, LoRa is preferable to RPMA in direct comparison for the present scenario.

3 CONCEPT: LORA + AX.25 + IPV4 + TCP

In [29], a data link layer protocol - a variation of the X.25 protocol - is specially adapted for amateur radio and specifies, inter alia, the communication via frames [5]. It is mainly used for ‘Packet Radio’, which is to be understood as the sending and/or receiving of digital data packets between two end devices via a radio channel. If more than one device participates, it is also called a ‘packet radio network’. AX.25 performs typical data link layer tasks such as establishing a connection between two end devices or providing wireless channel access.

For packet radio communication using AX.25, a modem connected to a ‘Terminal Node Controller (TNC)’ is required. This serves as an interface between the terminal device and the modem by means of a serial connection. End devices in an AX.25 network either communicate directly with each other or can be arranged in any topology. If the radio signals of two terminals do not reach each other due to too great a distance, they can be forwarded to the destination by one or more digipeaters, which, however, requires a-priori knowledge of the topology. The ‘Carrier Sense Multiple Access with Collision Resolution (CSMA/CR)’ method is used to control access to the radio channel. To identify subscribers, a six-digit ‘call sign’ ID is specified as the MAC address. Correspondingly, an AX.25 frame contains at least one source/destination address for addressing and, in the case of source routing using digipeaters, the addresses of the respective intermediate stations.

Since the current specification follows the OSI model, it is possible to use a variety of higher layers. For example, this is utilized by the ‘AMateur Radio Network (AMPRNet)’, where TCP/IP is used as a transport and network layer together with AX.25 as a data link layer. Since 1981, an entire class-A network is available for the use of IP in amateur radio networks with the regulated 44.0.0.0/8 address block, of which some blocks have been sold so far. The reserved private class-C address block 44.128.0.0/16 is, however, open to any amateur radio operator. To send AX.25 frames to a TNC via serial interface, a protocol is required. Nowadays, the ’Keep It Simple, Stupid (KISS)’ protocol is most commonly used for this purpose, which was developed primarily for the use of IP over AX.25 [9]. The flexibility of the OSI model for higher layers also applies to the physical layer in AX.25, as shown in Figure 1. Thus it would be possible to use a LoRa modem with suitable firmware for a TNC and hence enable TCP/IP communication via LoRa. Accordingly, only TCP/IP capable (legacy) systems would be available for direct integration into a network. This concept is to be implemented and carried out in the next step.

1 Physical Layer	2 Data Link Layer	3 Network Layer	4 Transport Layer	5 Session Layer	6 Presentation Layer	7 Application Layer
LoRa	AX.25	IPv4	TCP	HTTP, SSH, ...		

Figure 1: Concept of LoRa + AX.25 + TCP/IPv4 in the OSI Model

3.1 Test Bed: IP-Communication via LPWAN

For the purpose of evaluation, we implement the concept in the form of a test bed that should allow TCP/IP communication over LoRa. Regardless of the explicit test set-up, some components are needed to realize the test bed. First, the actual modem that supports the selected LoRa technology is required to establish a wireless connection. The modem, on the other hand, is typically embedded in a micro-controller platform. This platform can then be used to equip gateways with it so that they can establish a wireless connection via LoRa. Finally, two arbitrary terminal devices are needed that communicate with each other via TCP/IP.

Modem. LoRa is a technology patented by Semtech. Accordingly, LoRa modems are only available directly from Semtech or from licensed companies such as HopeRF. With the SX1260/1270/1300 chip family, Semtech has several LoRa modems that differ mainly in the supported bandwidth and frequency. In this work, a modem with the Semtech SX1276 chip is used [12]. This supports the frequencies released in Europe and offers a link budget of up to 168 dB with a low power consumption of 9.9mA during the reception.

Micro-controller. In order to use a LoRa modem, a micro-controller is needed to drive and control it. Generally, any platform can be used that allows an appropriate connection of the modem, for example, by means of UART pins. Further peripheral components complete the platform. This includes the SMA board for the connection of an antenna. For this work, the micro-controller ATmega1284P from Microchip is used. It offers 128 kB programmable flash and 1k kB RAM. As developer board, the RNode (see Figure 2) from unsigned.io is used [31], which offers a USB port for communication. The selection is justified by the fact that this board offers the most mature firmware for a required KISS-TNC.

Gateways. To communicate with two RNodes via TCP/IP, each node must be connected to a gateway. For the gateways, any hardware can be used that has a USB port, supports a Linux distribution, and offers an additional network interface such as LAN or WLAN. For portability reasons, a virtual machine (VM) is used for the first gateway. The resources of a VM can also be changed to runtime so that it is possible, among other things, to extend it with any network adapters and networks. Debian 10.3.0 is used as the operating system. For reasons of mobility, a laptop is used for the second gateway.

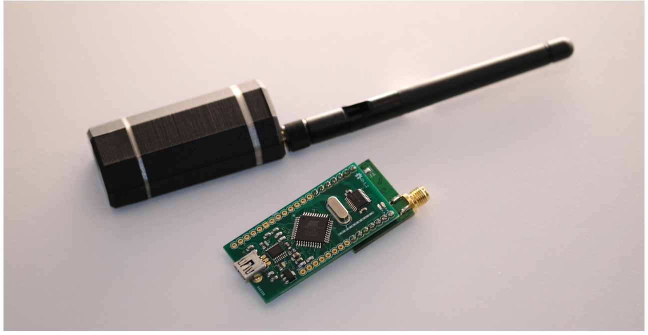


Figure 2: One RNode with case and the plain circuit board

End Devices. To demonstrate and evaluate the concept, two end devices are needed that communicate with each other using TCP/IP. These are implemented as VMs for the same reasons as the first gateway. Here, the flexibility of the operating system and the associated software offer also play a major role.

4 STUDY DESIGN

The utilized hardware has to be structured and arranged in a network topology. The following Figure 3 shows the individual components, required networks, and IP addresses of the test setup:

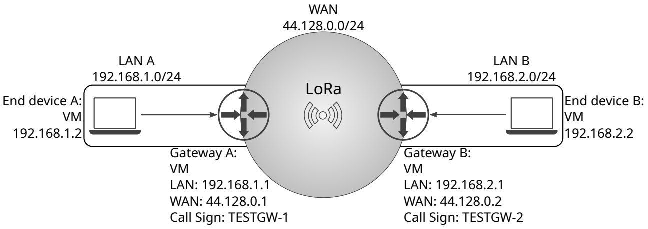


Figure 3: Schematic Illustration of Test Setup

If end device A wants to communicate with its counterpart B, the data is first sent to the local gateway A. The gateway knows a route to LAN B via gateway B and routes the data accordingly via the LoRa AX.25 WAN link. Gateway B finally forwards the data to end device B as the final destination. Vice versa, the same process applies to communication from B to A.

The described experimental setup is varied by the following parameters:

Distance. To test the range of the LoRa AX.25 WAN link in the existing hardware constellation, three different distances are to be covered in line-of-sight, resulting in three series of tests, as shown in table 4:

LoRa Parameters. As already discussed, LoRa can be influenced by the parameters frequency, spreading factor, bandwidth, and coding rate [2]. The frequency used is 869.4 MHz for all settings. The frequency is not varied due to radio regulation. The maximum duty cycle of 10% is possible in the bands between 869.4 and 869.65 MHz, so a frequency within this range was chosen. For the remaining parameters, three different constellations are described below, which,

Table 4: Test Series

	Aim	*Distance [m]*
Series A	feasibility	10
Series B	medium range functionality	100
Series C	long range functionality	1,000

similar to the test series, are intended for short, medium, and long distances, respectively, as shown in table 5:

This provides 9 combinations of test series and LoRa settings.

4.1 Implementation

Since the required AX.25 packages are not included by default in the Linux distributions being used, they must first be post-installed on both gateways:

```
# sudo apt install libax25 ax25-apps ax25-
    tools
```

The next step is to configure the AX.25 Data Link Layer. The following entry is added to the file `/etc/ax25/axports`:

```
ax0 TESTGW-X 115200 484 5 LoRa Gateway
```

Here, 'ax0' stands for the name of the AX.25 port and 'TESTGW-X' for the AX.25 call sign ID, the X having to be replaced correspondingly with gateway A by 1 or with B by 2. The number '115200' represents the baud rate, '484' represents the MTU, and '5' represents the window size. These values are specified by the platform firmware used, only the window size can be changed. However, since this is used by the platform developer, no changes are made. The last option serves as a free description text.

When the data link layer is ready for use, the network adapter can be configured. The file `/etc/network/interfaces.d/ax0` is created for this purpose and provided with the following static IP settings:

```
iface ax0 inet static
    address 44.128.0.X
    netmask 255.255.255.0
    network 44.128.0.0
    broadcast 44.128.0.255
    pre-up kissattach /dev/ttyUSB0 ax0
    post-down pkill -9 kissattach ; rm -f /
        var/lock/LCK..ttyUSB0
```

Here, in the same manner as further above, the 'X' must be replaced by 1 or 2 respectively.

Now it is necessary to connect the RNode platforms to one of the gateways via USB. Usually these are available under the file `/dev/ttyUSB0`. In order for an RNode to function as TNC, it is necessary to put it into TNC mode. For this, the 'RNode Configuration Utility' [32] can be used with the following command:

```
# sudo ./rnodeconf /dev/ttyUSB0 -T --txp 17
    --freq 869400000 --bw 250 --sf 7 --cr 1
```

The parameter 'T' is required to place the RNode under `/dev/ttyUSB0` in TNC mode and 'txp' for setting the radio strength in dBm. Subsequently, the frequency is given through 'freq', followed by the setting 'bw' for the bandwidth. Finally, the spreading factor is determined with 'sf' and the chip rate is being set with 'cr'. Depending on the LoRa setting, the command must be adjusted accordingly.

It is then possible to make the Linux network interface available under the name ax0:

```
# sudo ifup ax0
```

The command in the pre-up operation causes the USB-connected RNode to be used as TNC and initialized from the 'axports' file with the previously defined setting named ax0.

From this stage on, it is possible for the two gateways to communicate with one another via their respective network interface ax0. Static ARP entries help to reduce network load. In order to enable terminals of the different networks which are also connected to LAN ports to communicate with one another, routes to the respective LAN network must be introduced to the gateways. To expand the ARP/routing table of Gateway A accordingly, the arp or ip configuration tool is being applied:

```
[root@GatewayA ~]# arp -s -H ax25 44.128.0.2
    TESTGW-2
[root@GatewayA ~]# ip r add 192.168.2.0/24
    via 44.128.0.2
```

For gateway B, the command reads:

```
[root@GatewayB ~]# arp -s -H ax25 44.128.0.1
    TESTGW-1
[root@GatewayB ~]# ip r add 192.168.1.0/24
    via 44.128.0.1
```

In order for the Linux Kernel to route the received IP packets, the associated functionality must finally be activated on both gateways:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

At the very last, the static IP settings must still be made on the terminals in accordance with the mapping of the test setup. Since this is different, depending on the terminal and operating system used, and does not represent any challenge, it will not be discussed in detail.

5 RESULTS

In order to obtain unadulterated results, the measurements are carried out with the two gateways. The regular network parameters data rate, latency, and packet loss are measured for the combinations of test series/LoRa settings. This results in a total of 9 measuring points for each network parameter, providing a total of 27 measurements.

Data Rate. To determine the data rate, the frequently used open-source software iperf3 for network measurements is being applied. iperf3 is realized through a client / server application, so that a gateway displays the iperf3 server and the other combines to this as client.

First, iperf3 version 3.1.3 is launched in the verbosen TCP-server mode on gateway A and the report interval on two seconds is set:

```
[root@GatewayA ~]# iperf3 -s -V -i 2
```

Table 5: LoRa Settings

	Application Scenario	*Spreading Factor*	*Bandwidth [MHz]*	*Coding Rate*
Setting 1	short distance, high data rates	7	250	1
Setting 2	medium range, lower data rate	9	125	1
Setting 3	maximum range and reliability	12	125	1

Table 6: Measurements - Test Series A, 10 Meter

	Data Rate [kbps]	*Latency* [ms]	*Packet Losses* [#packets]
LoRa-Setting 1 (SF=7; BW=250 kHz; CR=1)	4,30	385,928	0
LoRa-Setting 2 (SF=9; BW=125 kHz; CR=1)	1,02	1322,451	0
LoRa-Setting 3 (SF=12; BW=125 kHz; CR=1)	0,0547	8471,749	0

Table 7: Measurements - Test Series B, 100 Meter

	Data Rate [kbps]	*Latency* [ms]	*Packet Losses* [#packets]
LoRa-Setting 1 (SF=7; BW=250 kHz; CR=1)	4,31	384,037	0
LoRa-Setting 2 (SF=9; BW=125 kHz; CR=1)	1,02	1322,658	0
LoRa-Setting 3 (SF=12; BW=125 kHz; CR=1)	0,0543	8471,936	0

Table 8: Measurements - Test Series C, 1,000 Meter

	Data Rate [kbps]	*Latency* [ms]	*Packet Losses* [#packets]
LoRa-Setting 1 (SF=7; BW=250 kHz; CR=1)	4,08	382,778	2
LoRa-Setting 2 (SF=9; BW=125 kHz; CR=1)	1,02	1323,771	3
LoRa-Setting 3 (SF=12; BW=125 kHz; CR=1)	0,0552	8472,444	1

To launch the measurement, the verbose iperf3 client mode is executed on Gateway B with the following command:

```
[root@GatewayB ~]# iperf3 −c 44.128.0.1 −V
```

Depending on the LoRa setting and distance, it is necessary to limit the number of bytes to be transmitted, otherwise the transit times become too long. This can be influenced with the parameter 'n', so instead of time-based transfer with the following command 10240 bytes data are transferred:

```
[root@GatewayB ~]# iperf3 −c 44.128.0.1 −V
    −n 10240
```

Latency and Packet Loss. To determine the latency and the number of lost packets, the 'Internet Control Message Protocol (ICMP)' and the application 'ping' contained in the operating system are inserted. For TCP latency measurements, applications such as nuttcp or qperf are also available, which, however, cannot run with all LoRa settings. Instead of measuring the packet loss of the TCP protocol, it can already be determined at IP or ICMP level. The micro-controller platform offers relatively little RAM and buffer for the TCP protocol compared to fully developed gateway hardware, therefore a packet loss could be due to these circumstances. In order to measure the quality of the link and not to explore the hardware limits, the packet loss is therefore determined without the TCP.

To get an empirical average, the number of sent ICMP packets is increased to 100, and the operation is started with the following command:

```
[root@GatewayB ~]# ping −c 100 44.128.0.1
```

Thereafter, Gateway B begins sending sequential ICMP echo requests to Gateway A. After receiving the ICMP echo response from Gateway A, the complete circulation time of the ICMP packet pair is issued as the measurement result.

For higher transit times, it is necessary to adjust the default setting of the timeout and transmission interval, otherwise incorrect measurements will likely occur. For a timeout of 10 seconds using parameter 'W' and a transmit interval of 10 seconds with parameter 'i', the command reads:

```
[root@GatewayB ~]# ping −c 100 44.128.0.1 −W
    10 −i 10
```

Results of the different test series measurements are shown in three Tables 6, 7 and 8. In the results of the data rate and latency, the measured values each reflect the mean value of the test.

As can be derived from the measurements, the LoRa radio connection is stable at 10 meters with all settings since no packet losses have occurred. The maximum data rate and minimum latency are achieved with LoRa-Setting 1. LoRa-Setting 3, which is explicitly intended for large distances, provides the lowest data rate and highest latency values. The measurement results show that even at 100 meters the radio connection is stable for all settings since no packet loss has occurred. From the results of the 1,000 meter test series, it can be deduced that the radio connection has some packet losses. However, these are so small that the radio connection can be regarded as fairly stable. The lowest packet loss is seen in LoRa-Setting 3, which, however, provides the worst data rate and latency. It could be concluded from this that the LoRa-Setting 1 is preferable since it has the best values on average.

As can be followed from the measurements, the LoRa-Settings have a decisive influence on data rate, latency, and packet loss. The settings differ in the spreading factor and partly in bandwidth, with a constant coding rate of 1. The LoRa-Settings 2 and 3, which differ

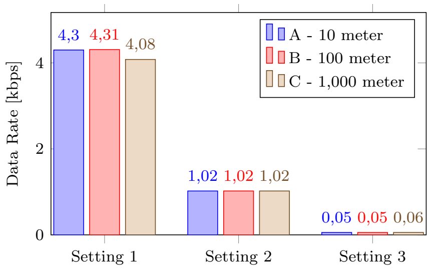


Figure 4: Measured Transfer Rates

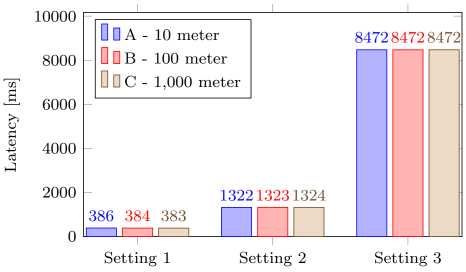


Figure 5: Measured Latency

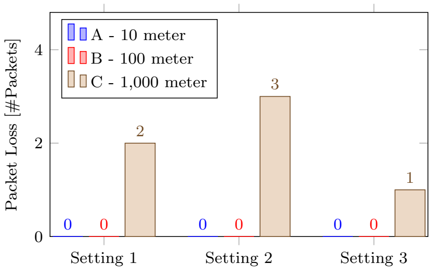


Figure 6: Measured Packet Loss

only in the spreading factor, indicates that changes on these level have an impact on the measured data rate and latency.

The Figures 4, 5, and 6 illustrate the relationship of the individually measured parameters to the respective LoRa settings for each test series.

The correlation between transmission time and different packet sizes is illustrated in figure 7. The bandwidth and coding rate are the same as LoRa-Settings 2 and 3. The figure reveals that an increase in the spreading factor is accompanied by a reduction in the data rate or, conversely, an increase in the transmission time required. The calculated values can be derived directly from the LoRa technology. The document 'LoRa Modulation Basics' from Semtech is available for this purpose, which contains a detailed derivation [11].

6 DISCUSSION

The selection of measurement applications showed that, for example, `nuttcp` or `qperf`, especially with low throughput and high latency as given with LPWAN technologies, do not work reliably and could be optimized for these. Operating system standard tools such as ping or netcat, on the other hand, prove to be fully functional even under these conditions with certain parameters. Special measurement applications for LPWAN and similar technologies would be desirable.

The slight variations in the measured values from different test series and one LoRa setting in particular illustrate the long-range character of the technology and the potential for bridging long ranges. In general, the fluctuations are within normal measurement tolerances, although at 1,000 meters, the somewhat larger deviations could be attributed to interference factors in the measurement path. In general, LoRa-Setting 1 delivers the best-measured values in all test series. Since even at the largest tested distance of 1,000 meters, the measured values are similar or equal to those of the previously tested distances, it can be concluded that much larger ones could be bridged. This is also consistent with the researched ranges of the physical layer comparison from section 2.

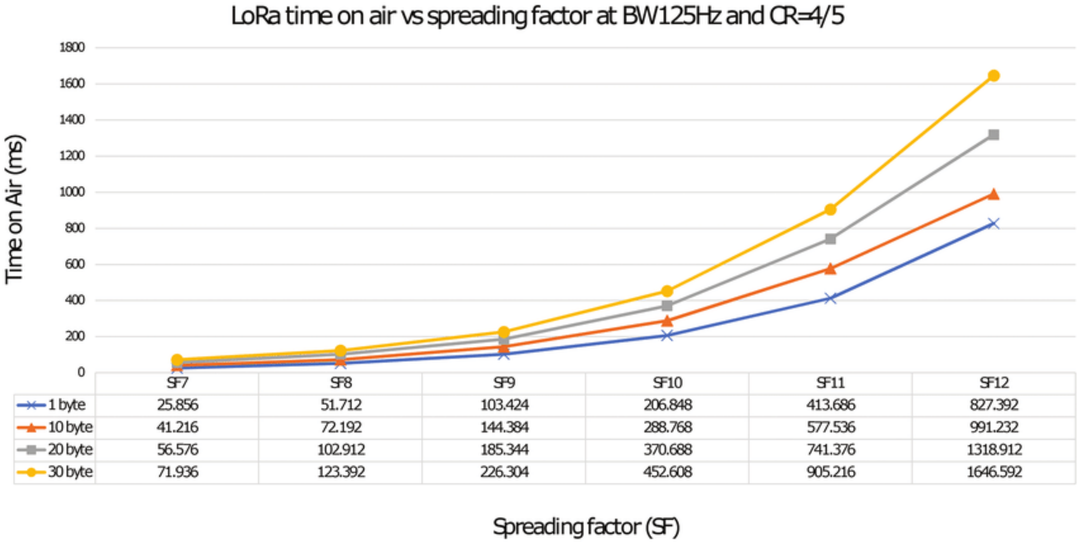
The successfully tested functionality of TCP and application protocols such as HTTP and SSH enables a whole range of different scenarios for monitoring or operating IT systems relevant to operational security in the event of a local crisis. In the case of HTTP, it is particularly noticeable that it remains functional in principle even with the low data rate and high latency of LoRa-Setting 3. In principle, the data rates achieved should also be sufficient for other application protocols based on TCP, such as the text-based protocols Telnet or SMTP/IMAP. Database connections or file transfers via FTP are also possible scenarios.

The limits of the test bed can be seen in the hardware used, among other things. The RNode developer platform has only very limited capacities and buffers, which are particularly important for the TCP protocol due to the connection orientation. Since the associated firmware is mainly developed by a single person and is intended for test purposes, it also has its limits when dealing with TCP. Whether a special application is ultimately functional with the concept or with technologies that have a low throughput and high latency depends on the protocol used and the individual application behavior, such as hard-coded timeouts. Another limitation is the SMA antenna with dimensions of only L105 × W10 × H10 mm. Especially at very large distances, an exchange is necessary in order to continue to exploit the range advantage of LoRa technology and to ensure a more stable connection [30]. Height positioning also plays an important role. For the same reasons, the height used in the test bed for positioning the antenna should be further increased by approx. two meters for large distances.

The tested application protocols, hardware components, and the test bed itself consequently hold potential for optimization. For HTTP, it is advisable to utilize the cache mechanisms contained in the protocol. If the requested data has not changed, this saves having to retransmit data when pages or functions are called, so that applications respond faster or better overall. Besides, the use of the SSH protocol can also be optimized. Continuous performance could be further increased by appropriate hardware. A platform with sufficient computing power and memory for buffers, as well as improved firmware optimized for TCP, could additionally increase the data rate. For long distances, as is common in agricultural fields, the range can be optimized by appropriately dimensioned and height-positioned antennas. However, even with the small antenna used, an increase is still achievable at 1,000 meters, as the technical evaluation shows.

7 CONCLUSION AND FUTURE WORK

The research question that we posed in Section 1 is as follows: *In times of increasing digitalization in agriculture, how can reliable data transmission to minimize or partly avoid the effects of local crises (outages of the internet/mobile network, radio gaps) with regard to operational safety-relevant processes, be realized?* To give an answer to this question, we firstly developed a concept based on our assessment of requirements and available (technical) options. Our



	SF7	SF8	SF9	SF10	SF11	SF12
1 byte	25.856	51.712	103.424	206.848	413.686	827.392
10 byte	41.216	72.192	144.384	288.768	577.536	991.232
20 byte	56.576	102.912	185.344	370.688	741.376	1318.912
30 byte	71.936	123.392	226.304	452.608	905.216	1646.592

Figure 7: Calculated LoRa Airtime vs. Spreading Factor, Source: [13]

concept allows the usage of *classic* IP-based communication protocols via a LoRa communication channel. This could be useful, e. g., to create redundant data transmission for critical information, like error messages of cattle shed air-ventilation systems, or to connect multiple stakeholders in cases of an Internet outage. Both examples of use could be mission-critical for the food production of an agricultural company. An implementation in the form of a test bed was able to confirm the general feasibility of our concept for different application protocols, distances, and settings.

Of interest would be further investigations of LoRa technology in the context of TCP. This includes the optimization potential of the test bed mentioned in the discussion. Since the full range potential of LoRa technology is not yet exhausted in the test bed, it would be of further interest to explore the limits with the given hardware. Also the AX.25 protocol supports more features, like so-called 'digipeaters', that allow packet forwarding over several hops, so even greater distances could be bridged than possible with a point-to-point connection. The development of a KISS/TNC firmware for more powerful hardware platforms would also be desirable, thus allowing more test scenarios to be evaluated that do not fail due to hardware or firmware limitations. Last but not least, the point of IT security could also be considered specifically for the scenario of critical infrastructures and their communication channels. In the future, it can be assumed that research will look at other IP-based solutions for LPWAN technologies and focus more on TCP since marketable solutions already exist for UDP. Thus, similar to the SCHC technology designed for UDP, which is currently still being standardized at the IETF, a variant for TCP would be conceivable. It remains uncertain which of the LPWAN technologies will prevail in the future within agriculture and in which protocol composition. However, it has been shown that LoRa technology is a promising candidate for this.

ACKNOWLEDGMENTS

This work was supported by funds of the German Government's Special Purpose Fund held at Landwirtschaftliche Rentenbank in the project Geobox-II as well as by the German Federal Ministry for Education and Research (BMBF) in the project HyServ (01IS17030B). A preliminary, earlier and much shorter version of this paper has been presented at the 41. GIL-Jahrestagung in March 2021 [22].

REFERENCES

[1] Giuseppe Aceto, Alessio Botta, Pietro Marchetta, Valerio Persico, and Antonio Pescapé. 2018. A comprehensive survey on internet outages. *Journal of Network and Computer Applications* 113 (2018), 36–63.

[2] Aloÿs Augustin, Jiazi Yi, Thomas Clausen, and William Townsley. 2016. A study of LoRa: Long range & low power networks for the internet of things. *Sensors* 16, 9 (2016), 1466.

[3] J. Bardyn, T. Melly, O. Seller, and N. Sornin. 2016. IoT: The era of LPWAN is starting now. In *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference*. 25–30. https://doi.org/10.1109/ESSCIRC.2016.7598235

[4] Luis Barreto and Antonio Amaral. 2019. Smart Farming: Cyber Security Challenges. *9th International Conference on Intelligent Systems 2018: Theory, Research and Innovation in Applications, IS 2018 - Proceedings* (2019), 870–876. https://doi.org/10.1109/IS.2018.8710531

[5] William A Beech, Douglas E Nielsen, Jack Taylor Noo, and Lee Knoper Ncuu. 1997. Ax. 25 link access protocol for amateur packet radio, version: 2.2 rev. In *Tucson Amateur Packet Radio Corp.* Citeseer.

[6] Isaac Brown. [n.d.]. A Detailed Breakdown of LPWAN Technologies and Providers. http://web.luxresearchinc.com/hubfs/Insight_Breakdown_of_LPWAN_Technologies.pdf

[7] Bundesministerium des Innern. 2016. Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV). In *Verordnungdes Bundesministeriums des Innern*, Vol. 3. 248.

[8] Himadri Chaudhary, Honey Patel, and Birju Tank. 2018. Comparative Analysis of Internet of Things (IoT) based Low Power Wireless Technologies. *International Journal of Engineering Research* 7, 01 (2018).

[9] Mike Chepponis and Phil Karn. 1987. The KISS TNC: A simple Host-to-TNC communications protocol. In *6th Computer Networking Conference*, Vol. 225. 06111–1494.

[10] Cagdas Civelek. 2017. Low power wide area network (lpwan) and internet of things adaptation in agricultural machinery. *Scholars Journal of Agriculture and Veterinary Sciences* 4, 1 (2017).

[11] Semtech Corporation. 2015. AN1200.22 LoRa Modulation Basics. https://www.semtech.com/products/wireless-rf/lora-core/sx1276

[12] Semtech Corporation. 2020. Semtech SX1276/77/78/79 Datasheet Rev. 7. , 132 pages. https://www.semtech.com/products/wireless-rf/lora-core/sx1276

[13] T Durand, Lourens Visagie, and M.J. (Thinus) Booysen. 2019. Evaluation of next-generation low-power communication technology to replace GSM in IoT-applications. *IET Communications* (07 2019), 1. https://doi.org/10.1049/iet-com.2019.0168

[14] Stephen Farrell. 2018. Low-Power Wide Area Network (LPWAN) Overview. *Internet Engineering Task Force (IETF)* (2018).

[15] Sonia Gul, Jairo Gutierrez, Nurul I Sarkar, and Edmund Lai. 2018. RESILICOMM: A Framework for Resilient Communication System. *Proceedings of ISCRAM Asia Pacific* (2018), 1–5.

[16] Matthias Herlich and Ferdinand von Tüllenburg. 2018. Introduction to Narrowband Communication. In *Wireless Congress: Systems and Applications*. 1–15.

[17] Jonas Höchst, Lars Baumgärtner, Franz Kuntke, Alvar Penning, Artur Sterz, and Bernd Freisleben. 2020. LoRa-based Device-to-Device Smartphone Communication for Crisis Scenarios. In *17th International Conference on Information Systems for Crisis Response and Management*, Amanda Hughes, Fiona McNeill, and Christopher W. Zobel (Eds.). ISCRAM, 996–1011.

[18] IoT Analytics GmbH. 2018. LPWAN Market Report 2018-2023. https://iot-analytics.com/product/lpwan-market-report-2018-2023/

[19] Tom Martin Jung. 2017. Vergleich aktueller LPWAN-Technologien im Internet der Dinge unter Einbindung von Energy-Harvesting. https://opus.hs-offenburg.de/frontdoor/deliver/index/docId/2297/file/TomJung_Bachelorthesis_final.pdf

[20] Rajat Kathuria, Mansi Kedia, Gangesh Varma, Kaushambi Bagchi, and Richa Sekhani. 2018. The anatomy of an internet blackout: measuring the economic impact of internet shutdowns in India.

[21] Sandra Koenig and Stefan Schauer. 2019. Cascading Threats in Critical Infrastructures with Control Systems. *Proceedings of the 16th ISCRAM Conference* 16 (2019), 1252–1259.

[22] Franz Kuntke, Marcel Sinn, Sebastian Linsner, and Christian Reuter. 2021. Low Power Wide Area Networks (LPWAN) für krisentaugliche Datenübertragung in landwirtschaftlichen Betrieben. *41. GIL-Jahrestagung, Informations-und Kommunikationstechnologie in kritischen Zeiten* (2021). https://dl.gi.de/bitstream/handle/20.500.12116/35671/GIL2021_Kuntke_193-198.pdf

[23] Sebastian Linsner, Franz Kuntke, Enno Steinbrink, Jonas Franken, and Christian Reuter. 2021. The Role of Privacy in Digitalization – Analysing the German Farmers' Perspective. *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2021, 3 (2021), 333–349. https://doi.org/10.2478/popets-2021-0050

[24] Philipp Lottes, Raghav Khanna, Johannes Pfeifer, Roland Siegwart, and Cyrill Stachniss. 2017. UAV-based crop and weed classification for smart farming. In *2017 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 3024–3031.

[25] M Madhumitha and Bhupendra Pratap Singh. 2017. A survey on LPWAN technologies in content to IoT applications. *ICT Express* 3, 1 (2017), 14–21.

[26] Kais Mekki, Eddy Bajic, Frederic Chaxel, and Fernand Meyer. 2018. Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 197–202.

[27] Kais Mekki, Eddy Bajic, Frederic Chaxel, and Fernand Meyer. 2019. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* 5, 1 (2019), 1–7.

[28] Thomas Muenzberg, Ulrich Berbner, T. Comes, Hanno Friedrich, Wendelin Gross, Hans-Christian Pfohl, and Frank Schultmann. 2013. Decision Support for Critical Infrastructure Disruptions: An Integrated Approach to Secure Food Supply. *Proceedings of the 10th International ISCRAM Conference* 10 (2013), 312–316.

[29] Keith Nolan and Mark Kelly. 2018. IPv6 Convergence for IoT Cyber–Physical Systems. *Information* 9, 4 (2018), 70.

[30] Mark Qvist. 2018. 15 kilometre LoRa SSH link with RNode. https://unsigned.io/15-kilometre-ssh-link-with-rnode/

[31] Mark Qvist. 2018. RNode. https://unsigned.io/projects/rnode/

[32] Mark Qvist. 2018. rnodeconfigutil. https://github.com/markqvist/rnodeconfigutil

[33] Ylli Rama and M Alper Özpmar. 2018. A Comparison of Long-Range Licensed and Unlicensed LPWAN Technologies According to Their Geolocation Services and Commercial Opportunities. In *2018 18th Mediterranean Microwave Symposium (MMS)*. IEEE, 398–403.

[34] Usman Raza, Parag Kulkarni, and Mahesh Sooriyabandara. 2017. Low power wide area networks: An overview. *IEEE Communications Surveys & Tutorials* 19, 2 (2017), 855–873.

[35] Christian Reuter, Wolfgang Schneider, and Daniel Eberz. 2019. Resilient Smart Farming (RSF)–Nutzung digitaler Technologien in krisensicherer Infrastruktur. *39. GIL-Jahrestagung, Digitalisierung für landwirtschaftliche Betriebe in kleinstrukturierten Regionen-ein Widerspruch in sich?* (2019).

[36] Eli Rohn and Gil Erez. 2012. Fighting Agro-Terrorism in Cyberspace: A Framework for Intention Detection Using Overt Electronic Data Sources. *Proceedings of the 9th International ISCRAM Conference* 9 (2012), 1–5.

[37] Minwoo Ryu, Jaeseok Yun, Ting Miao, Il-Yeup Ahn, Sung-Chan Choi, and Jaeho Kim. 2015. Design and implementation of a connected farm for smart farming system. In *2015 IEEE SENSORS*. IEEE, 1–4.

[38] Laura K Schüller and Wolfgang Heuwieser. 2016. Measurement of heat stress conditions at cow level and comparison to climate conditions at stationary locations inside a dairy barn. *Journal of Dairy Research* 83, 3 (2016), 305–311. https://doi.org/10.1017/S0022029916000388

[39] Xiaojie Shi, Xingshuang An, Qingxue Zhao, Huimin Liu, Lianming Xia, Xia Sun, and Yemin Guo. 2019. State-of-the-art internet of things in protected agriculture. *Sensors* 19, 8 (2019), 1833.

[40] Lorenzo Vangelista, Andrea Zanella, and Michele Zorzi. 2015. Long-range IoT technologies: The dawn of LoRa™. In *Future Access Enablers of Ubiquitous and Intelligent Infrastructures*. Springer, 51–58.

[41] Wenbo Wang, Stefan L Capitaneanu, Dana Marinca, and Elena-Simona Lohan. 2019. Comparative analysis of channel models for industrial IoT wireless communication. *IEEE Access* 7 (2019), 91627–91640.

[42] Sjaak Wolfert, Lan Ge, Cor Verdouw, and Marc-Jeroen Bogaardt. 2017. Big data in smart farming–a review. *Agricultural Systems* 153 (2017), 69–80.

[43] Rongtao Xu, Xiong Xiong, Kan Zheng, and Xianbin Wang. 2016. Design and Prototyping of Low Power Wide Area Networks for Critical Infrastructure Monitoring. *IET Communications* 11 (12 2016). https://doi.org/10.1049/iet-com.2016.0853