Received: 3 September 2021 | Revised: 3 December 2021 | Accepted: 3 January 2022

DOI: 10.1002/ett.4452

RESEARCH ARTICLE

WILEY

LoRaWAN security issues and mitigation options by the example of agricultural IoT scenarios

Franz Kuntke | **Vladimir Romanenko** | **Sebastian Linsner** | **Enno Steinbrink** | **Christian Reuter**

Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt, Darmstadt, Germany

Correspondence to:
Franz Kuntke, Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt, Darmstadt, Germany.
Email:kuntke@peasec.tu-darmstadt.de

Funding information
Bundesministerium für Bildung und Forschung, Grant/Award Number: 01IS17030B; Deutsche Forschungsgemeinschaft, Grant/Award Number: 251805230/GRK 2050; Landwirtschaftliche Rentenbank, Grant/Award Number: GeoBox-2, AgriRegio

Abstract

The Internet of Things (IoT) is a major trend that is seen as a great opportunity to improve efficiency in many domains, including agriculture. This technology could transform the sector, improving the management and quality of agricultural operations, for example, crop farming. The most promising data transmission standard for this domain seems to be *Long Range Wide Area Network (LoRaWAN)*, a popular representative of low power wide area network technologies today. LoRaWAN, like any wireless protocol, has properties that can be exploited by attackers, which has been a topic of multiple research papers in recent years. By conducting a systematic literature review, we build a recent list of attacks, as well as collect mitigation options. Taking a look at a concrete use case (IoT in agriculture) allows us to evaluate the practicality of both exploiting the vulnerabilities and implementing the countermeasures. We detected 16 attacks that we grouped into six attack types. Along with the attacks, we collect countermeasures for attack mitigation. Developers can use our findings to minimize the risks when developing applications based on LoRaWAN. These mostly theoretical security recommendations should encourage future works to evaluate the mitigations in practice.

1 | INTRODUCTION

The Internet of Things (IoT) is a hot topic with various use cases, which are usually prefixed by the term *smart*, like *smart home*, *smart city*, and *smart farming*. The idea of IoT is to use networks ("internet") to connect sensor devices or actor devices ("things") with information technology (IT) systems. This allows for monitoring or automated controlling of the environment in the real world. One essential component of each IoT system is the data transmission technology. Depending on the use case, the requirements for wireless transmissions differ. Smart home solutions may just have to bridge a couple of meters to the next gateway. But in other scenarios, this can be a lot different—the distance to the next gateway can be many meters (smart city) or even kilometers (smart farming). Wireless transmission protocols that suit this long range requirement for IoT applications are grouped by the term low power wide area network (LPWAN), covering several network protocols from different vendors, for example, LoRaWAN, SigFox, NB-IoT, LTE-M. Compared to more traditional wireless network protocols like Wi-Fi, LPWAN protocols allow for a much higher transmission distance between devices, up to several kilometers, as well as having a low power consumption.[1] The most popular solution—at least in the domain of agriculture—seems to be LoRaWAN, a specification designed by the LoRa Alliance.[2] In comparison with the direct alternatives, LoRaWAN achieves a lower power consumption (ie, higher battery life) alongside support for rather high data transfer rates while embedding authentication and encryption by default.[3]

With the increased use of IoT systems using LoRaWAN for data transmission, the risk of malicious participants taking advantage of any vulnerabilities of the LoRaWAN technology also increases. Therefore, a specific analysis of attacks on LoRaWAN as one promising protocol for IoT is necessary.

Since LoRaWAN has existed for several years now, surveys[4,5] inspecting the protocol's security were already conducted to some extent. However, in the time between those surveys were conducted, more vulnerabilities were detected, and the LoRa Alliance has published new LoRaWAN versions that affect the vulnerability to some of the older attacks. Therefore, this article will provide a recent survey on the security of LoRaWAN. To illustrate use cases and attacks, we choose agricultural IoT applications as we see rather challenging use cases (from a security perspective) here that combine many properties which demand LPWAN solutions like LoRaWAN. But the findings will also hold for LoRaWAN applications of other domains. The research questions (RQ) of this work are:

RQ1: *What are the known vulnerabilities of LoRaWAN?*
RQ2: *Which mitigations against the known vulnerabilities should be considered when developing a LoRaWAN-based IoT solution?*

To answer these questions, we first outline some IoT applications in the use case of agriculture to give an idea of how IoT applications work and which requirements make LPWAN, for example, LoRaWAN, necessary. By conducting a systematic literature review, we extract domain specifics as well as known LoRaWAN vulnerabilities.

By providing a comprehensive list of countermeasures to reduce the vulnerability of an (agricultural) IoT setup, we aim to help developers and scientists to employ LoRaWAN applications. Developers that aim to work on an IoT project may be the main beneficiaries of this article. The contributions are the following:

- overview of the LoRaWAN technology,
- a review of IoT specifics for wide area applications (considering agricultural IoT as an example),
- a recent overview of vulnerabilities of LoRaWAN and its mitigations, and
- security recommendations for IoT application developers using LoRaWAN.

The structure of the article is as follows: Section 2 gives background information about LoRaWAN and the state of research. Section 3 provides specifics of IoT applications that require wide area transmissions, using the example of agriculture. Section 4 describes the literature selection method. In Section 5, the selected literature is used to list the vulnerabilities of LoRaWAN setups. In the same section, preventive mechanisms are proposed for each attack—primarily from the perspective of an IoT application developer. Section 6 presents the discussion, and Section 7 concludes the article.

2 | BACKGROUND AND RESEARCH GAP

2.1 | Overview about LoRaWAN

The LoRa Alliance*published the LoRaWAN protocol standard, which is primarily used for connecting battery-powered end-devices, like environmental sensors. This protocol is popular in industry and science, which may be due to the fact that it combines a high range with acceptable bandwidth and comparatively low cost.[6] At the time of writing, v1.0.4[7] (released in 2020) and v1.1[2] (released in 2017) are the two suggested protocol specifications for new developments. But when looking at commercially available end-devices, it seems that the former standards LoRaWAN v1.0.2 (released in 2016) and v1.0.3[8] (released in 2018) are dominating—unfortunately, such devices cannot be easily upgraded as there are different hardware requirements for v1.1 and v1.0.4.

According to the specifications, a typical LoRaWAN network consists of the following components: end devices (EDs), also called *nodes*, gateways (GWs), network servers (NSs), join servers (JSs) and, application servers (ASs) (see Figure 1). EDs communicate with GWs, and GWs forward raw data frames to the NS over standard IP connections, for example, via Ethernet or cellular data connections. The NS is responsible for validating and decoding packages, as well as forwarding

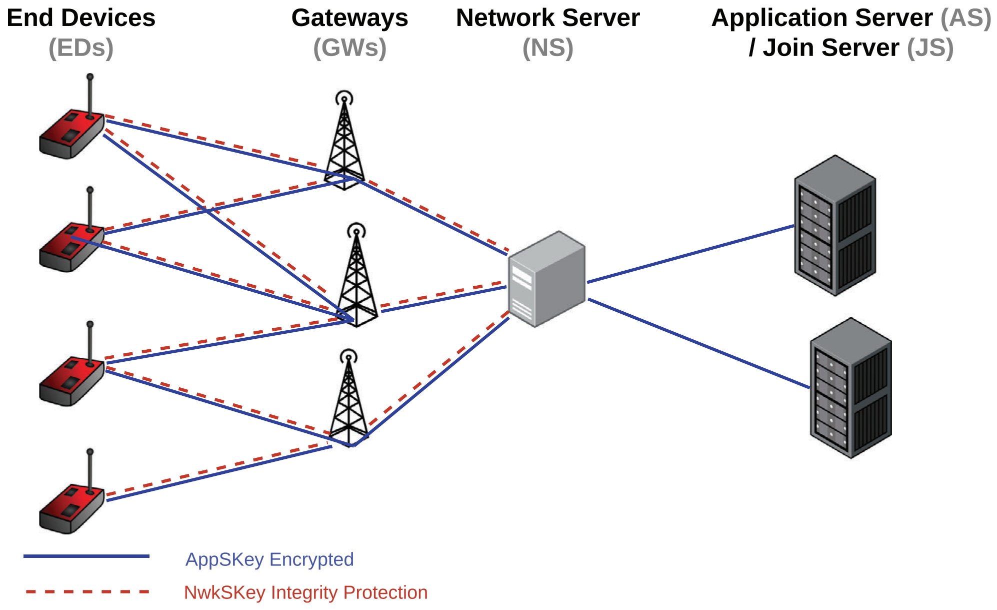

FIGURE 1 LoRaWAN architecture and key usage (own illustration)

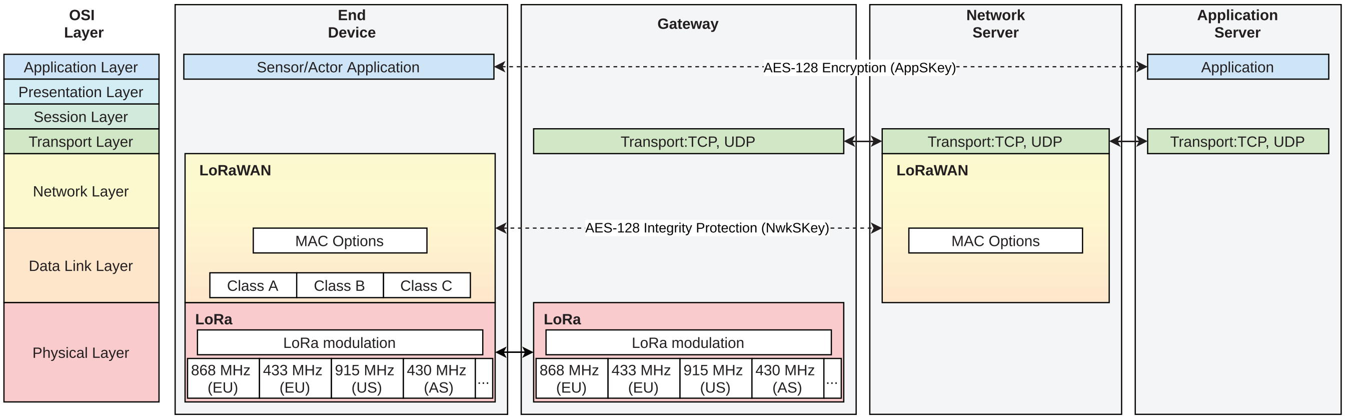

FIGURE 2 Simplified LoRaWAN technology stack in the OSI model (own illustration)

them to the AS. It also manages other LoRaWAN features like the adjusting adaptive data rate (ADR). The communication between an ED and a GW is done via the LoRa specification (physical layer and data link layer). When considering the Open Systems Interconnection (OSI) model, LoRa is filling the physical layer and LoRaWAN forms the data link layer and the network layer (see Figure 2). LoRa uses a wireless modulation utilizing the chirp-spread spectrum[9] for transmission.

Khutsoane et al[10] present an overview of (scientific) applications of LoRa and LoRaWAN, for example, measuring urban greenhouse gas emissions, monitoring the temperature of blood fridges, and water grid management. The physical layer LoRa can also be used without the LoRaWAN part (data link layer and network layer) for different use cases, like wide-area point-to-point communication[11] or communication devices for network outage scenarios.[12] But in this present paper, we concentrate on the rather common usage of LoRaWAN in terms of IoT setups.

2.2 | LoRaWAN specifics

The LoRaWAN specification[7] defines three ED classes: Class A, Class B, and Class C. These three classes differ in the frequency of open receive window time slots, which has a direct impact on the power consumption and battery life.

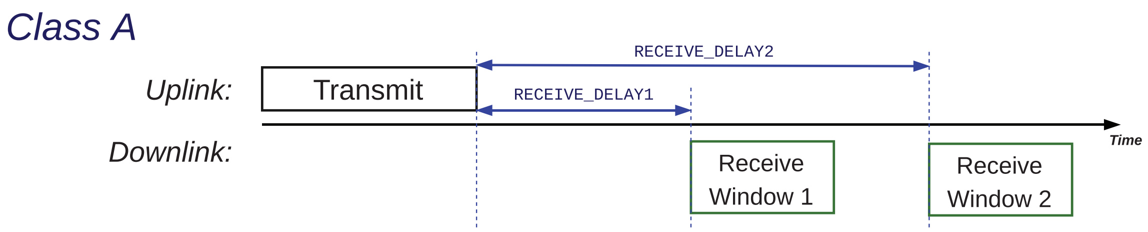

FIGURE 3 Class A ED receive-slot timing (own illustration)

- *Class A* can send data at any time (uplink), but the other direction from the NS towards the ED (downlink) is restricted. There are up to two short downlink receive windows, followed by each uplink transmission (see Figure 3). For this reason, all downlink communications from the NS must wait until an uplink is initiated by the ED.
- *Class B* differs from Class A by having more and scheduled receive slots. In order for the Class B-enabled EDs to open the extra receive windows at scheduled times, it receives a time-synchronized beacon from the gateway. In this case, the NS knows when the ED is listening and must not schedule the downlink message for an ED to an ED-initiated transmission. Battery consumption is higher compared to Class A-enabled EDs.
- *Class C* goes one large step further and has continual receive windows. Class C-enabled EDs listen almost continuously for downlink messages. The receive windows are just closed during the transmission of an ED. Obviously, having the radio device listening all the time consumes more energy, and, therefore, the battery life is shortest with Class C-enabled EDs.

The topology of LoRaWAN networks is “star-of-stars,” where one NS can talk with multiple GWs, and each GW can communicate with multiple EDs. An NS forwards packets received by one or more GWs to the responsible AS and vice versa. There is no hard relation between an ED and a specific GW. If an uplink transmission by an ED is received by multiple GWs, all GWs forward the LoRaWAN packet to the connected NS, which performs *deduplication* of the multiple receptions of the same packet. In case a downlink transmission should be sent to an ED, the NS chooses the GW for transmission.

LoRaWAN transmissions use two session keys for safeguarding a message’s security and integrity (see Figure 1): The `AppSKey` is used to end-to-end encrypt the payload between ED and AS via Advanced Encryption Standard (AES). The integrity of messages between an ED and an NS is ensured by integrating message integrity codes (MICs) in the transmitted packets, calculated via AES-CMAC.

The `AppKey` is the personalized, unique 128-bit AES root key of each ED that must be pre-configured by the device manufacturer. Based on this `AppKey`, the session key `AppSKey` is derived during the ED activation process.

2.2.1 | Device activation schemes

For registering an ED, two activation modes exist: Activation By Personalization (ABP) and Over-The-Air Activation (OTAA). In both modes, the desired ED is provisioned with three keys: a device address (`DevAddr`), a network session key (`NwkSKey`), and an application session key (`AppSKey`). When using ABP, all three individual keys are directly stored on the ED before it can participate in the LoRaWAN network. In the specifications of LoRaWAN v1.0.4 and v1.1, it is recommended to use OTAA for “higher security applications.” When using OTAA, all EDs must be personalized with a global unique ED identifier (`DevEUI`), the JS identifier (`JoinEUI`), and an AES-128 root key `AppKey`. The `AppKey`allows the derivation of the session keys `NwkSKey` and `AppSKey` when the device joins via OTAA.

2.2.2 | LoRaWAN specification history

The first specification was released with *LoRaWAN v1.0* in January 2015. *LoRaWAN v1.0.1* was introduced in February 2016 with some minor changes and clarifications of the specifications. *LoRaWAN v1.0.2* was introduced in July 2016 and added the encryption of the Uplink Frame Counter (`FCntUp`) and added this counter (`FCntUp`) to the confirmation messages (ACK downlinks) as a preventive measure against replay attacks. Starting with that release, regional parameters were also shipped as a separate document. *LoRaWAN v1.1* was introduced in October 2017 with many drastic changes that place higher requirements on ED hardware as well as new software requirements on NS. JS and NS are separated—prior, the functions were managed solely by the NS. Frame counters could not be reset, two keys (texttNwkKey, texttAppKey) for session security were introduced. *LoRaWAN v1.0.3* was introduced in July 2018, bringing some changes of v1.1 into the v1.0.x branch, mainly for Class B devices. *LoRaWAN v1.0.4* was introduced in October 2020 with more changes and clarifications. But as there are also new hardware requirements (persistent storage for `FCnts`), it can be seen as a breaking change.

2.3 | Security issues of LoRaWAN

Several studies have examined the LoRaWAN protocol and found various security gaps depending on the respective version. Aras et al[13] focused on LoRaWAN's physical layer (LoRa) and have shown that it is possible to jam a LoRa network using commercial off-the-shelf hardware. Another work that focuses on LoRaWAN security by Yang et al[4] presents five possible attacks to compromise confidentiality, availability, or integrity and provides a selection of countermeasures. Some known attacks have since been addressed by the release of LoRaWAN v1.1. This version introduced many security-related changes together with the option to support backward compatibility for v1.0. However, as investigated by Dönmez and Nigussie,[14] only session key derivation is addressed when using the backward compatibility mode—other security benefits are lost. Their work is the first to provide a full list of detailed attacks for both of the supported LoRaWAN versions. A similar list has been compiled by Butun et al[5] for LoRaWAN v1.1 only, but it lacks detailed attack information and security recommendations, which we aim to provide within this work. Especially with the release of LoRaWAN v1.0.4, we have not found any security review of LoRaWAN that takes into account the changes of this protocol version.

2.4 | Research gap

Several scientific papers recommend more research on IoT security in general, as well as in specific domains like smart farming.[15-17] Unfortunately, it is currently difficult for developers or researchers to obtain simple, clear security recommendations for the development of IoT solutions in general and more difficult when it comes to the specific use scenario of agriculture. Another problem is the variety in today's deployed and actively used IoT technologies and protocols. In this work, we focus on LoRaWAN, as it seems to be popular in science and industry—and also in agriculture.[18,19] Even though LoRaWAN is just a couple of years old (v1.0 was released in 2015), multiple works that collate security issues exist.[4-6] With the publication of more vulnerabilities, as well as new LoRaWAN specification releases, we see the need for an updated overview about security issues, as well as mitigation options.

The overall goal of this work is to provide a list of possible LoRaWAN attacks and to provide security recommendations that are not reliant on protocol changes and are therefore usable by developers working in the field. As an example for attack illustration, we choose the agricultural IoT environment, as this example allows to argue for multiple requirements in one use case. The following section (Section 3) collects IoT specifics on the example of agricultural applications.

3 | SPECIFICS OF IOT IN WIDE AREA APPLICATIONS

This section presents specifics of IoT in applications that must cover large areas, as LoRaWAN is especially for those use cases a relevant technology. We have chosen agriculture as a tangible example for listing example applications of IoT and for rendering known attacker profiles by real-world use cases with a demand for IoT security.

3.1 | Specifics of wide area IoT by the example of agricultural applications

According to the American Heritage Dictionary of the English Language,[20] agriculture is the *"science, art, and business of cultivating soil, producing crops, and raising livestock."* It is an essential part of the food chain and responsible for feeding the world's population. Therefore, agriculture is typically considered to be a critical sector and should be treated as such.

For that reason, all the necessary technologies and tools of agriculture must be designed carefully with regard to safety and security.

There are many kinds of specific agricultural businesses that are part of agriculture, for example, livestock breeding, viticulture, crop farming. In this article, we take conventional crop farming as our exemplary IoT use case, as we see both a trend in increasing offers for crop farming specific smart devices and also an increasing demand for high efficient production that requires modern technologies, like IoT networks deployed in large areas. In the following, we list specifics building on contributions of multiple publications,[16,21-30] where (a), (b), (c) are rather relevant for the success and applicability of attacks and (d), (e) are rather influencing the motivation of adversaries:

(a) Physically accessible devices When looking at the surveillance of sensor/actuator units set up on the area of operation (agricultural fields), the majority of these EDs must be considered *unsupervised* without specific safety mechanisms, that is, an attacker might easily access and modify it.[22]

(b) Area of operation We have to deal with potentially large areas between connected devices, as this is may be one reason to choose LoRaWAN. As rural areas are rather sparsely populated, usually, there are not any or just a few electronic devices between EDs. Additionally, IoT devices are potentially exposed to harsh environmental phenomena.[22]

(c) Lack of IT knowledge The end-users (eg, farmers) should not be treated as IT experts with knowledge about specifics of IT security[24,27,31] as well as IoT specifics.[21] Facing an heavy workload, the farmers' time budgets are limited.[32,33] Therefore, agricultural IoT solutions need to be ready to use without difficult and time-consuming manual steps.

(d) Sensing and acting Devices used in IoT scenarios are both sensors and actuators. In agriculture, sensors are used for weather conditions, supervision of plant growth, nutrition, and water level. They generate the data that are the basis for a decision, like how many fertilizers could be applied or what is the optimal water inflow. Controlling the water flow of an irrigation system is an example use case for actuators.[23,28,30] Especially the potential modification of the environment makes agricultural IoT use cases worthy of protection.

(e) Increasing responsibility of single companies As for social responsibility, we see a trend that fewer companies (eg, farms) are responsible for supplying more people (eg, with food), at least in the western world.[25,26] This is due to the increased operational performance though the use of more precise methods and further improvements in technology.

3.2 | Security of IoT systems on the example of agricultural applications

Different works have investigated possible benefits and challenges for IoT in agriculture, with Elijah et al[21] stating that they believe the adoption rate will increase in the following years. However, the authors warn that additional research in security is required to ensure continued growth. Barreto and Amaral[34] support this statement, showing the importance of IT security across the software and hardware landscape in agriculture by drawing high-level scenarios like *agroterrorism*, the agricultural branch of cyber terrorism. One given example concerns the malicious manipulation of smart farming devices in a way that may lead to a refusal of the produced food by the food supply chain. The threat of malicious misinformation is further highlighted by Gupta et al.[16] In their overview of smart farming and general security threats, the authors cite the flooding of a field by feeding erroneous data into the system as an example of such an application.

Demestichas et al[17] give an overview of more general security threats in agricultural IoT and also grouped applications into seven areas. We take their grouping and give examples of ED that could be used to fulfill the application in Table 1.

3.2.1 | Attacker description

The focus of our work is on the wireless link between ED and GW and the physical access on the EDs itself. In the following, we use the terminology and proposed attacker profiles for cyber-physical systems by Rocchetto and Tippenhauer[35] and tailor these profiles to the agricultural IoT use cases by adjusting the profiles for the context of agricultural IoT:

The *basic user* is the attacker profile without a clear target of harming a specific company, but with time and interest to understand the technique. This profile includes hobbyists that want to see how things work and could also be a threat to agricultural IoT by having fun to exploring technologies like LoRaWAN in a rather offensive manner, comparable to war-driving. Their monetary budget is limited, but they have quite a lot of time for experiments.

The profile *insider* includes people with a lot of knowledge about concrete installed setups. In the case of agricultural IoT, this profile matches (past) employees of IoT service providers who installed IoT setups on the field. Their motivation

TABLE 1 Agricultural IoT application area according to Demestichas et al[17] with ED examples

IoT application area	Example
Continuous land monitoring	Surveillance cameras
Water management	Smart valves or pumps
Monitoring and reporting of crop growth	Cameras
Identification and management of soil characteristics	Sensors for temperature, humidity, and light
Detection and recognition of diseases in crops and/or plants	Optical sensors on leafs of a representative plant; multi-spectral cameras on multicopters for big areas
Enhanced food preservation and quality control	Gas, temperature, and humidity sensors
Smart livestock	Smart collars for cattle

could be to discredit the IoT service provider by disturbing the IoT setups on the field. Their time and money budget is limited, but they have insider information, for example, which device is accessible on which position.

Hacktivists could especially be a problem in agriculture, as debates about environmental threats often include agricultural practice. Their time and money budget is rather high, and also the knowledge could be treated as high.

The *terrorism* profile does not match too well with the agricultural IoT scenario we consider in our article. Although there is a general threat to the domain by agrifood-terrorism, we see just a low motivation for attacking single IoT setups, but rather attacks on the cloud-domain of much-used software, which is not in the scope of this present paper.

Agricultural IoT could also be of interest to *cybercriminals*, especially when considering bigger farms with a bigger financial pad that could be the target of attacks (eg, Denial-of-Service (DoS)) in combination with blackmailing.

Like *terrorism*, we did not see *nation-state* attackers as a real danger for the scope of this article, as this attacker profile usually aim for greater targets and less on single IoT setups.

4 | LITERATURE SELECTION METHOD

This section describes the method that formed the upcoming section: the systematic literature review[36,37] for collecting vulnerabilities and mitigations specific to LoRaWAN (Section 5).

The questions for the literature review are:

Q1: Which attacks or vulnerabilities exist for LoRaWAN (and LoRa)?
Q2: Which mitigations exist to prevent known vulnerabilities for LoRaWAN (and LoRa)?

We selected the following keywords to build our search string:

- LoRaWAN, LoRa
- Vulnerability, Attack
- Security, Cybersecurity, Mitigation.

Based on the keywords we built the search string: `(~LoRaWAN~ OR ~LoRa~) AND (~Vulnerability~ OR ~Attack~) AND (~Security~ OR ~Cybersecurity~ OR ~Mitigation~)`. The following databases/publishers served as data sources: ACM Digital Library , IEEE Xplore , Science@Direct , Springer , Taylor and Francis . After performing the queries on the databases, we collected 403 articles. Further filtering was done based on:

- Inclusion criteria:
  - Published in between 2015 and 2021
  - Describes at least one attack, vulnerability, or mitigation
  - Provides technical details of the attack, vulnerability, or mitigation.

- Exclusion criteria:
  - Not peer-reviewed
  - Not published in English
  - No relation to LoRa (WAN).

After filtering based on these criteria, we obtained 37 articles (Table 2) we used for the compilation of vulnerabilities and mitigations (Section 5).

5 | VULNERABILITIES AND MITIGATIONS

This section compiles the collected vulnerabilities of LoRaWAN, which we found through the previously literature selection (Section 4). The presentation includes an attack procedure to increase understanding and special cases, which might not be immediately apparent for some selected attacks. As no found literature inspected the most recent LoRaWAN v1.0.4 (see Table 2), we checked the specification[7] for having the same characteristics that made the described attack working. Additionally, within each attack, we include an assessment of the potential impact on confidentiality, integrity, and availability, such as that used by the CVSS Impact Metric[71] to evaluate various attacks. Subsequently, known countermeasures to prevent or reduce the impact of the attacks are proposed for each attack type. We roughly grouped the attacks based on the attack type in Figure 4. A listing of all countermeasures together with the mitigated attacks is presented in Table 3.

5.1 | Physical attacks

Being placed out in the open and lacking any strong physical protection, EDs can be subjected to multiple direct, physical attack options—especially in agriculture; this is a serious threat. Those options can be grouped into the following three attacks:[39] *(a) ED destruction, removal, or theft*, *(b) Security parameter extraction*, and *(c) ED cloning or firmware replacement*. All of these attacks are not specific for LoRa devices but important to consider when designing a robust system. Being agnostic to the transmission data technology, the attacks are possible in each version of the LoRaWAN specification.

(a) *ED destruction, removal, or theft*. Destruction, removal, or theft of an ED limits the information available to the system by disabling a responsible ED. While theft is only possible by a malicious entity, multiple sources for device damage or removal exist, for example, environmental effects, animals, or destruction by humans due to an accident—to name some of the more likely ones. It is important to note that this list is incomplete as other sources of device damage might exist depending on location.
For IoT in agriculture, this attack presents a high threat for availability, permanently removing an ED from the system and forcing additional replacement costs. However, the attack has no effects on confidentiality and integrity.

(b) *Security parameter extraction*. An attacker with physical access on an ED can attempt to extract security parameters. A serial interface, if available on the ED, can be used to extract all key exchanges due to the lack of built-in encryption between the host microcontroller and radio module in contemporary radio modules. However, such an attack would only comprise data stored in the specific ED, as root keys are uniquely generated. Nonetheless, this can be combined with firmware replacement to allow the reuse of keys.[5,40]
Security parameter extraction would allow an attacker to read all data sent by the ED, and represents a clear threat for confidentiality, however, the impact is low in agriculture. As mentioned earlier, root keys are unique, and most of the data from a single sensor can be accessed using other methods, or is not enough to disclose relevant business information. Extracting security parameters in itself provides no threat for availability or integrity.

(c) *Firmware replacement*. Physical access can also be used to intercept all data exchange between the host microcontroller and the radio module and use this information to create a mock device with the same credentials. The attacker could also resort to advanced tampering to potentially modify or replace the firmware, which could lead to key reuse being possible.[5]

This is the most dangerous of all the physical attacks. Allowing for key reuse allows an attacker to potentially obtain information from many sensors and leak business secrets like soil composition, we therefore rate the impact as high for confidentiality. Furthermore, an attacker could use the replaced firmware to feed any data into the controlling subsystem,

TABLE 2 Detected publications of the systematic literature review, together with the referenced LoRaWAN version, and described attack-types, according to our categorization (Figure 4)

Author, year	Referenced LoRaWAN version	Described attack-type
Lee et al[38]	v1.0	Other (MitM)
Na et al[39]	v1.0	Message Replay
Aras et al[40]	v1.0	Physical, Message Replay, DoS
Tomasin et al[41]	v1.0	Message Replay, DoS
Aras et al[13]	v1.0	DoS
Kim and Song42, [42]	v1.0.2	Message Replay
Gladisch et al[43]	v1.1	Message Replay, Traffic Analysis
Yang et al[4]	v1.0.2, v1.1	Message Replay, DoS
Sung et al[44]	Not defined	Message Replay
Danish et al[45]	Not defined	DoS
Benkhala et al[46]	v1.0	Spoofing, Other (MitM)
Skorpil et al[47]	v1.0.2, v1.1	Message Replay, Spoofing, Other (MitM)
Cheng et al[48]	Not defined	*No described attack*
Dönmez and Nigussie[14]	v1.0.2, v1.1	Message Replay, Traffic Analysis, DoS, Spoofing, Other (MitM)
Butun et al[5]	v1.1	Message Replay, Traffic Analysis, DoS, Other (MitM)
Mundt et al[49]	v1.1	Message Replay
van Es et al[50]	v1.0.2, v1.1	DoS
Ruotsalainen and Grebeniuk[51]	v1.1	Traffic Analysis
Coman et al[52]	v1.0.1, v1.0.2, v1.0.3, v1.1	Other (Packet Forging)
Wadatkar et al[53]	v1.0	DoS
Raad et al[54]	v1.1	Other (MitM)
Xu et al[55]	v1.0.3	Other (Side-Channel)
Hill et al[56]	Not defined	DoS
Saxena et al[57]	Not defined	DoS
Kamble and Gawade[58]	Not defined	DoS, Other (MitM)
Eldefrawy et al[59]	v1.0, v1.1	Message Replay, DoS
Mikhaylov et al[60]	v1.1	DoS
Bala et al[61]	v1.0	*No described attack*
Thomas et al[62]	v1.1	Other (MitM)
Philip et al[63]	v1.0, v1.1	DoS
Gu et al[64]	v1.0.2	DoS
Perković and Siriščvić[65]	v1.1	DoS
Singh et al[66]	v1.0	DoS
Noura et al[67]	v1.0.1, v1.0.2, v1.0.3, v1.1	Physical, Message Replay, Traffic Analysis, DoS, Spoofing, Other (MitM)
Hessel et al[68]	v1.0.2, v1.0.3, v1.1	Spoofing
Wang et al[69]	Not defined	Spoofing
Lv et al[70]	Not defined	Message Replay

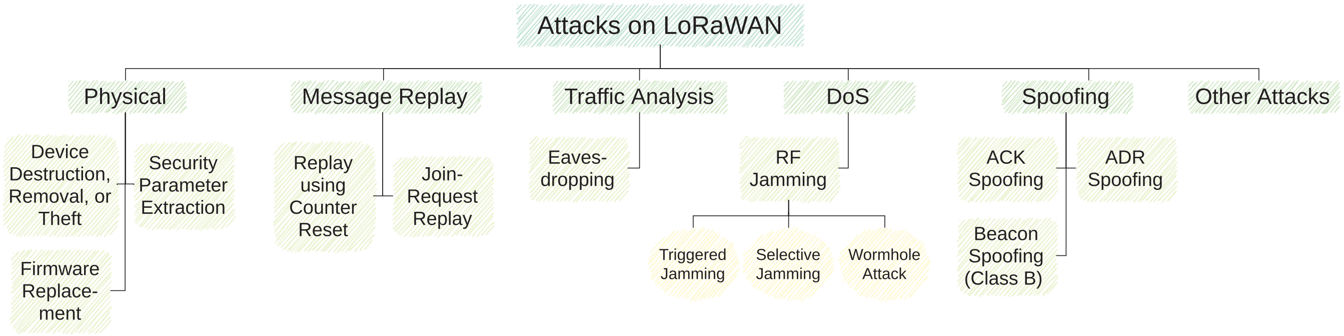

FIGURE 4 Attack types of the LoRaWAN vulnerabilities (own illustration)

TABLE 3 Tabular listing of countermeasures, together with the scope of application, related (vulnerable) LoRaWAN versions and mitigated attacks. (v1.1* is v1.1 in backward compatibility mode)

	LoRaWAN version			Scope			
Countermeasure	**v1.0**	**v1.1***	**v1.1**	**ED**	**GW**	**NS**	**Mitigation for**
Traffic analysis	x	x	x			x	RF jamming
Multiple GWs with overlapping coverage	x	x	x		x		RF jamming ADR spoofing
Monitoring SNR values	x	x	x			x	ADR spoofing
Physical protection (EDs)	x	x	x	x			Physical attacks
Physical protection (GWs)	x	x	x		x		Class B attacks ACK spoofing (≤ v1.0.3)
Keeping multiple unconfirmed messages per ED	x	x		x			Join-request replay
Ending session with OTAA when counter saturated and force re-keying	x	x		x		x	Replay Attack Eavesdropping
Avoiding ABP	x	x		x			Replay Attack Eavesdropping (≤ v1.0.3)
EDs resend mission critical messages	x			x			ACK spoofing (≤ v1.0.3)

which could prove fatal when dealing with automated irrigation for example. We therefore rate the impact on integrity as high as well. A firmware attack that modifies the sensor to produce gobbled data is equivalent to removing it from the system entirely in regards to availability and is classified as high, similar to the destruction-based physical attacks described earlier.

5.1.1 | Countermeasures against physical attacks

Physical attacks are a problem for the IoT world as some usage scenarios do not allow EDs to be physically protected from unauthorized third parties. Ways to mitigate physical access like surveillance via cameras and hiding through unobtrusive design are known, but some strategies can help to further reduce the impact of such attacks:

(a) To ensure authentication and integrity of the software, the firmware should be verified using ultra-low-power cryptographic hash functions.[5] Also secure hardware elements could enhance the security level against physical attacks.[67]

(b) EDs should be checked routinely for unauthorized hard- or software modifications as well as damage.[72]
(c) Extracted cryptographic parameters will change upon initiating a new session when using OTAA, making extracted parameters useless. This is not the case for ABP, and, therefore, OTAA should be preferred.

5.2 | Message replay

5.2.1 | Replay using counter reset

There are two activation modes available in a LoRaWAN setup: *ABP* and *OTAA*. In ABP-mode, EDs use static keys that can't be changed for the duration of the EDs' lifetime. Non-volatile memory for frame counters that is allowed up to LoRaWAN v1.0.3[8] results in a vulnerability to replay attacks. In OTAA-mode, EDs are safe from replay attacks caused by manual devices resets but are still vulnerable to counter resets caused by overflowing as the session keys remain the same.[8]

The ED reset vulnerability can be abused by an attacker to replay messages from previous sessions, thereby withholding changes from the GW. Resetting the counter after an overflow can be used to replay pre-reset messages to de-synchronize the GW and ED counters and thereby cut the communication between those two.[2] An attacker has to monitor and store messages, which can be done in the radio range of GW and ED, but does not require knowledge of the exact location of either. Because the counter value is not encrypted during the message transmission, it is readable by eavesdropping the LoRaWAN transmissions. Additionally, counter values are also predictable since the counter is a sequence number, either encoded by 16bit (≤ v1.0.3) or 32bit (optional in ≤ v1.0.3, forced in v1.0.4/v1.1). After the counter resets (after an overflow or after a device reset in ABP-mode), the attacker can replay an old message that fits into a sliding window with a set up gap (default value of 16 384). All future messages that are received with a lower counter value are discarded on the receiving device. When replaying single messages that max out the sliding window borders, this procedure is basically a DoS attack.

In agricultural applications, an attacker can just drop a small malicious battery-powered device in the coverage area of both the targeted ED and GW for executing the attack. As the attack is dramatically improved in the time requirement by a manual device reset (in ≤ v1.0.3), physical access to an ED makes this attack more applicable, but also more expensive in terms of manual work. Therefore, we see here danger for the most critical single devices, for example, smart valves used for controlling water management. Such devices when under attack could be randomly manipulated in the water flow to obfuscate the attack.

Those attacks were addressed in LoRaWAN v1.1 due to the obligation of a persistent memory for counter storage and a re-join possibility to re-key the device during a running session. Nonetheless, it should be noted that re-keying is not possible when running in backward compatibility mode, making this attack a threat for a system relying on backward compatibility.[14]

When discussing the attack impact, we classify it as none for confidentiality, as no data is leaked. The impact on integrity is classified as high, because serious harm is possible, for example, by feeding incorrect data to an automated gate or a water pump. Although an attacker is limited in the ability to discern values due to encryption, the open location of the sensors and the ease of observing specific phenomena makes discerning important values easier than in other IoT domains. The impact on availability is low in our opinion, as it is possible to remove an ED by resetting the counter and replaying high counter value messages, but important data should most often be available from other sources due to the distributed nature of IoT systems in general.

Special case: Fake session creation

A fake session is possible between an attacker and an NS,[4] as well as between an attacker and an ED.[14] Both of those attacks exploit the weakness in `nonce` reuse and allow the attacker to proceed with a normal replay attack once the fake session is created. Both of those attacks are no longer possible in LoRaWAN v1.1 and only work in backward compatibility mode if the victim is the one running v1.0. Thus, a fake session on the ED is only possible if the ED is running v1.0.

Countermeasures against replay attacks

Both types of replay attacks are only possible for LoRaWAN v1.0 (and v1.1 in backward compatibility mode). Using LoRaWAN v1.1 would, therefore, solve this issue. For LoRaWAN v1.0 deployments, the following countermeasures can be performed to reduce the risk of being attacked:

(a) Prefer using OTAA. ABP uses static keys, and the counter will reset to 0 every time the device resets, which could be exploited by an attacker.
(b) Yang[73] advises protecting devices against physical access, as being able to reset the device manually can decrease the waiting period for an attacker attacking an ABP-activated device. Of course, in some use scenarios of agricultural IoT, physical protection is not possible to a sufficient degree.
(c) In a backward compatibility scenario, if the NS is v1.1 with a v1.0 ED, the NS should be configured to discontinue communication with an OTAA activated v1.0 ED upon recognition of a frame counter saturation to force the node to initiate another activation, as it is the only available way of re-keying, as described by Dönmez and Nigussie.[14]
(d) Another suggestion is discontinuing communication with an ABP-activated ED upon detecting a frame counter saturation. As re-keying is not possible, this approach results in additional costs as the ED needs to be replaced.
(e) Wang et al[69] suggested a solution *SLoRa* as an ED authentication scheme, that leverages two physical layer features: carrier frequency offset and spatial-temporal link signature. Based on the fingerprint-like transmission characteristics of each device, a new (malicious) ED could be detected at the GW side.

5.2.2 | Join-request replay

When using OTAA for activation, join-request messages are unprotected against replay attacks before LoRaWAN v1.1. The NS only stores most recently used `DevNonce` values, as repetition is possible due to the pseudo-random character. This can be abused by the attacker by replaying previously captured join-request messages, while the ED attempts to connect to the NS.

In the beginning, the attacker installs a sniffing device in the target area, for example, in the vicinity of a farmhouse, and proceeds to collect join-request messages from different EDs, aiming to acquire as many as possible. The second phase is about analyzing collected messages to determine EDs that send join-request messages frequently and regularly; those devices are the target of this attack. Additionally, the attacker stores the devices' expected join-request cycles, calculating the optimal time for an attack. Phase three starts when enough messages are collected, and the joining pattern of a given ED is figured out. Now, the attacker needs to wait for the usual device's join-time. Right before this moment, the attacker starts to replay the cached join-request messages. The NS attempts to connect to the attacker's device, as its message arrived first, discarding join-requests from the regular node. After a while, the timeout limit exceeds, and the NS drops the unconfirmed session. However, the attacker can replay the next cached join-request to restart the procedure until he runs out of cached messages.[14,39] This results in the ED being unable to participate in the network until all join messages have been used.

This attack is still possible when running in backward compatibility as a security context switch is not possible when one participating device is using LoRaWAN v1.0.[4,39]

It is hard to exclude agricultural application areas from this attack scope, but this attack will be easily detectable, as it hinders complete ED from joining the network, and there are no ways known for obfuscation of this attack.

The attack has no impact on confidentiality or integrity; no data in the system is disclosed or modified. Furthermore, the attack has a low impact on availability, being severely limited by the number of messages an attacker has captured, which happens the attack duration, as well as affecting a single ED only.

Countermeasures against the join-message vulnerability

This vulnerability relies on insufficient replay protection for join-request messages in LoRaWAN v1.0 versions. As the attack is not possible in LoRaWAN v1.1, using this version would solve the problem. If the system requires the usage of LoRaWAN v1.0, we recommend the following security measures that can be applied to reduce the impact:

(a) Avoiding clear patterns to server reboots and resetting devices at *random* times will make it impossible for the attacker to disconnect multiple devices at once, severely lowering the impact of the attack.
(b) Resort to block-chains for EDs' authentication in real-time could eliminate the attack possibility and build trust among LoRaWAN EDs and NSs.[74]
(c) Modifying the join procedure to account for potential replays while keeping the existing packet structure; an exemplary method using two types of join-requests is presented by Kim and Song.[42]

5.3 | Traffic analysis: Eavesdropping

LoRaWAN implements channel confidentiality through AES in counter mode, where the block counter value is used as an input. During a counter reset, the key will remain in place, meaning that the block cipher will recreate the same key material. An attacker can exploit this behavior to decrypt messages, as described by Yang et al.[4]

This attack is possible in LoRaWAN ≤ v1.0.3 due to the ability to reset the counter by restarting the device. In a second attack variant, the attacker exploits the lack of the `ForceRejoinReq` command, as the counter is resetting to 0 upon overflowing according to the specification.[14] Despite the attack variant, the attacker has just to monitor and store messages, which can be done in the radio range of GW and ED, but does not require knowledge of the exact location of either.

Eavesdropping can be combined with a replay attack to allow the attacker to replay specific messages based on his needs and feed erroneous data to the backend.

This attack is especially applicable for getting deep insights into a farm's operations by eavesdropping the results of the sensor nodes, for example, soil analysis sensors of arable farming businesses. In combination with the replay attack, this could be especially dangerous for modern food systems by introducing wrong data that manipulate calculations that determine the amount of applied fertilizer.

Considering the findings from the last paragraph, we classify the impact on confidentiality as low in the general case. However, as shown earlier, an attacker using background knowledge to target specific EDs could be able to obtain crucial business information, which in turn would raise the attacks impact to high. The attack itself has no impact on integrity or availability.

5.3.1 | Countermeasures against Eavesdropping

As Eavesdropping is only possible for LoRaWAN v1.0 (and LoRaWAN v1.1 in backward compatibility mode), using LoRaWAN 1.1 would solve this issue. In the case where the system has to contain LoRaWAN 1.0 components, the following countermeasures can be used to reduce the risk for an attack:

(a) Prefer using OTAA. ABP should only be used in special circumstances, as resetting the ED is the easiest way to obtain messages from the same node with the same session keys and the same counter value, which are required to derive keys used.[4] Physically protecting ABP nodes makes the attack much more difficult to perform as a counter overflow takes time to occur, and a considerable amount of messages with the same session key and counter value are required. This could be interesting for in-house sensors, like cattle monitoring. Especially actors (eg, smart locks, valve controllers) should not rely on ABP.
(b) When running in backward compatibility mode, implement a re-keying procedure without ways to reset the counter so the attacker can't perform an eavesdropping attack.

5.4 | Denial of service: Radio frequency jamming

Radio Frequency Jamming is one of the more general problems for IoT technologies. The adversary transmits a powerful radio signal in the proximity of the application devices, disrupting transmissions. In agricultural applications, this may be used to reduce or completely destroy the quality-of-service, applicable to all application areas of agricultural IoT. Motives could be the denunciation of a competing IoT-service provider or obtaining ransom money by criminals.

While such an attack is typically in need of dedicated hardware, Aras et al[13] as well as Perković and Siriščević[65] have shown that it is possible to jam LoRaWAN using commercial (low-cost) off-the-shelf hardware. This poses a real threat for LoRaWAN networks as throughput can be decreased by up to 56%.[75] The attack is possible for LoRaWAN v1.1 as well v1.0. We differentiate the following types of jamming attacks: *Triggered Jamming*, *Selective Jamming*, and *Wormhole Attack*.

(a) *Triggered jamming* can be used by the attacker to increase package loss in the network, in addition to providing a good basis for more sophisticated attacks like selective jamming. The technique is based on the functionality of LoRa radio modules to scan a certain channel to detect an ongoing transmission. Upon detection, the attacker can proceed with jamming.

(b) *Selective jamming* requires a low-level configuration to allow reading a message while it is being received. During the attack, the radio module starts in receiver mode and waits for a LoRa modulated signal. Once a message is detected and its physical header is proven correct, the module reads the FIFO until it reaches the device address. If the message triggers the jamming policy, the module switches to jamming mode. Once jamming is done, the module switches back to receiving mode again.[40] As this attack could be used to manipulate messages of single devices, there is a danger for the most critical EDs, for example, smart valves used for controlling water management. Such devices, when under attack, could be randomly manipulated to obfuscate the attack.

(c) A special case is the combination of selective jamming and a replay attack to perform a so-called *Wormhole Attack*. Two types of devices are required in this case, a *sniffer* capturing the packet and a *jammer* signaling the successful capture. The captured message can then be replayed at a later date since there is no time-related information in LoRaWAN messages. The attack is limited by the jammer's reaction time, which needs to be lower than the packet's airtime minus the airtime of the first five bytes of the device address; otherwise, the jammer will not have time to act before the packet reaches the gateway. This attack was addressed in v1.1 but is still possible in v1.0 versions and when running in backward compatibility mode.[40] We do not see specific attack scenarios for this attack in agricultural IoT applications.

The attack has no impact on confidentiality or integrity. However, the impact on availability is high, as the attacker is able to disconnect multiple EDs and is not limited by external factors like stored messages or specific timings.

5.4.1 | Countermeasures against jamming attacks

Jamming is limited by the number of nearby GWs, packet airtime, and channel hopping. Those limitations can be used to implement the following countermeasures:

(a) Creating a dense LoRa network with overlapping GW coverage makes a jamming attack much more difficult to perform. In this way, an attacker needs to make sure the message of an ED is not received by any of the different located GWs, as the success of the attack depends on physical proximity to the GW.[13,68] In case any GW receives the message of an ED, the message will be forwarded to the NS, which de-duplicates the message if multiple GW have received the same message. Of course, the feasibility to set up multiple GWs in distinct locations depends on the present circumstances on the farm. Another countermeasure is to maximize the use of channel hopping (usually used to reduce packet collision), which makes the jammer need to become more complex and expensive as it must listen to more channels at once.

(b) In the case of wormhole attacks, the signal frequency and the packet size can be lowered to reduce air-time and beat the jammers' reaction time.[13] It should be noted that a lowered signal frequency results in lower reliability and a lowered communication range.

(c) Mikhaylov et al[60] noted that network adaptation, for example, switching to a higher signal frequency or transmitting power, can be abused by an attacker to drastically increase energy consumption, thereby shortening the remaining device lifetime. As of now, there is no known solution. Hence, it should be considered when deploying IoT devices.

(d) A jamming attack may be detected by performing a traffic analysis at the GW or at the NS level. When there are regular transmission rates known, abnormal message quotas could be detected and trigger an alarm or a network adaption.[13]

5.5 | Spoofing attacks

5.5.1 | ACK spoofing

The attack exploits the lack of association between acknowledgment and message. The frame counter of the ACK is the sequential number of all downlink messages. Therefore, a captured and delayed ACK can be used to acknowledge another unrelated message without its arrival at the backend provider.[4]

An attacker will observe the network waiting for the NS to acknowledge any message from the ED. Afterward, the attacker will proceed to selectively jam the ACK message, capturing it in the process. Now the attacker can abuse the lack of association to be able to acknowledge any next single uplink message without its arrival at the backend by replaying the cached ACK. The ED then believes the message arrived and will not attempt to resend potentially mission-critical data. This attack can be used to prevent the communication of a status change of an actor, like a smart lock of a cattle farm, or water valve of an irrigation system.

This attack is possible in LoRaWAN v1.0 versions and was addressed in v1.1 by the changes to MIC calculation. However, this attack is still possible when running in backward compatibility mode.[4,14]

The attack reveals no information, and therefore it has no impact on confidentiality. The impact on integrity is low, as during modification of the data, the attacker is limited to single messages and hindered by encryption. The impact on availability is low as well; some messages are gobbled by the flip and unusable to the system. However, in an agricultural IoT system, it should be easy to recreate those missing data pieces.

Countermeasures against ACK Spoofing
Using LoRaWAN v1.1 would solve the issue. If the system requires LoRaWAN v1.0, the following countermeasures can be performed to reduce the risk of being attacked:

(a) Protecting access to GWs as the attack requires the adversary to be in control of the GW. A common method to attack a LoRaWAN gateway is using physical access.[4]
(b) Confirmed messages should be treated carefully, and EDs should be programmed to resend critical data or requests. Even if the message is acknowledged, the *critical* state remains.

5.5.2 | ADR spoofing

This attack forces an ED to use insufficient transmission power and data rate to reach a GW by manipulating ADR control messages, as described by Hessel et al.[68] The intention of LoRaWAN's ADR function is to find an appropriate data rate as a compromise of coverage and transmission time. By selective forwarding messages with a wormhole setup, an attacker is able to capture and jam the ADR initiating message, which was sent by an ED. This captured message can be manipulated in its metadata to fake the signal strength indicators, which are evaluated on the NS to calculate appropriate transmission parameters. By transmitting the ADR answer message back to the ED, the ED applies the transmission parameters, which are insufficient to reach the GW. As a result, the ED's coverage is too low to be able to communicate directly with the GW.

This attack has no impact on confidentiality or integrity because it does not leak or modify any data. However, the attack has a high impact on availability because it is possible to permanently disconnect EDs from the system, which in turn severely limits an agricultural IoT setup.

Countermeasures against ADR spoofing
This attack is also possible with LoRaWAN v1.1. Abandoning the ADR feature and manual setup of the network parameter would prevent this attack. Mitigating this attack could be achieved by monitoring the signal-to-noise-ratio (SNR) values and averaging the SNR at the NS to prevent abrupt changes.[68]

5.6 | Other attacks found in literature

There are additional attacks linked to LoRaWAN that can be found in the literature. The following attacks are presented for completeness, but we did not develop security recommendations for those attacks as they are either not possible to our knowledge or unspecific for LoRa/LoRaWAN devices. Nevertheless, developers have to also be aware of those vulnerabilities when developing any IoT application, regardless of the chosen technology.

(a) *Man-in-the-Middle (MitM)/Bit flipping*. LoRaWAN messages are encrypted and equipped with a MIC. However, these two layers of security (encryption and integrity check) are handled at different locations inside a message frame: The payload encryption is handled by the AS, while the MIC is checked and terminated by the infrastructure provider. *"This means that in between the infrastructure operator's network server and the IoT solution provider's application server, the content cannot be checked for integrity and authenticity,"* as stated by Yang et al.[4] An attacker can attempt to intercept anywhere between the NS and the AS.[38,47,62] This can be done via different approaches, ranging from routing-based ones, like BGP-prefix hijacking or IP source routing to physical and link-layer based ones, like a compromised device on the path. While normal AES is resistant to bit flipping due to the avalanche-effect, LoRaWAN is not using authenticated encryption and therefore terminates the integrity check too early. This allows the attacker to potentially modify the content of sensor readings and abuse the ciphertext, which affects the exact bit position in the plain text in a predictable manner.[4]

(b) *Side channel*. Xu et al[55] have demonstrated that based on electromagnetic radiation (EMR) of an ED and the knowledge about the communication mechanisms of the LoRaWAN protocol, the full `AppSKey` could be recovered with less than 100 transmissions in the ABP mode, utilizing neuronal networks (deep learning). To tackle EMR based attacks electromagnetic shielding like a Faraday cage around the computational hardware elements could be applied.

(c) *Class B device attacks*. There are three classes of LoRaWAN EDs described by the standard: class A, B, and C. While all EDs can send messages to a GW at any time, the class determines when an ED can receive messages from a gateway. Class A nodes are able to receive messages right after sending a message. Class C ("Continuous") nodes never sleep and always listen to incoming messages. Class B devices aim to balance power consumption with the possibility to receive messages periodically. However, they have a vulnerability: To open receive windows at fixed times, gateways need to broadcast a beacon synchronously to provide a time reference. As beacons messages contain GPS coordinates of the sending GW in plaintext, its position can be easily eavesdropped or spoofed when combining the attack with triggered jamming. Another class B attack is a *rogue beacon* that could be set up by the attacker and used to send random or extreme wakeup times to class B EDs. This leads to a distortion of receiving operations due to the device waking up at a different time than expected by a legitimate GW. Hessel et al[68] use this behavior for a *beacon spoofing* attack, which could result in a DoS.

(d) *Network flooding*. When attempting a network traffic flood, the adversary captures the EDs and misuse those to perform an attack against the rest of the network. Such an attack can degrade the network by flooding it with packages.[5]

(e) *Network traffic analysis*. A network traffic analysis is a passive attack where the attacker sets up a rogue GW and uses the received packages to deduce some knowledge about the data being transmitted or key material used.[5]

(f) *Self-replay attack*. To our knowledge, a self-replay attack is not possible but was referenced in another paper.[5] To our understanding, this was a misconception or mixing of properties of LoRaWAN and another LPWAN technology, *SigFox*. The latter one has a communication quota with a maximum number of messages per day.

6 | DISCUSSION

Multiple papers have investigated security aspects of LoRaWAN and have shown that, while LoRaWAN is a promising technology, it bears multiple issues independent of the application domain. The works by Yang et al[4] and Butun et al[5] are probably the most prominent works in this category, while the work of Noura et al[67] is the most recent survey, that covers multiple vulnerabilities, we have detected in our literature review. The result of our literature study shows that the newer the LoRaWAN 1.0 version, the fewer attacks are known. But also the newest 1.0 release (v1.0.4) has more known vulnerabilities compared to v1.1.

When looking at the attacks, some of the more dangerous vulnerabilities require or benefit from physical access to an ED, which is especially for agricultural IoT systems a real threat—in contrast to many other IoT use cases that have EDs deployed in physically protected environments, like buildings. When talking about attack complexity, we can see that almost all attacks exhibit a low complexity. For the most part, attacks can be performed with of-the-shelf hardware and rely on well-known and documented attack patterns; other attacks are easy to perform due to the ease of physical access inherent to the agricultural IoT domain. Another important aspect of IoT in agriculture is that none of the attacks we discovered require any kind of system privileges or legitimate user interaction. The scope of attacks varies while some attacks only affect a specific ED, others can harm the entire IoT system, for example, by feeding incorrect or potentially malicious data into an irrigation controlling system.

Unfortunately, multiple commercial EDs that are advertised for the agricultural sector like electric valves, soil moisture sensors, or general-purpose EDs, which could be equipped with different sensors or actors, are still delivered with LoRaWAN v1.0.2 or v1.0.3. We did not cover hints about possible firmware upgrades for the inspected products. Together with the promise to have a battery runtime of up to +10 years, this situation is critical from an IT security perspective.

This article is, to our knowledge, the first work that uses a systematic literature review to provide a full list of LoRaWAN vulnerabilities for the multiple versions up to v1.0.4 and gives security recommendations as countermeasures that do not require a change on the LoRaWAN standard itself. The tabular listing (Table 3) of countermeasures should help developers to minimize risks and improve IoT security.

6.1 | Limitations

The presented attacks and security recommendations are (only) based on documents of existing LoRaWAN specifications and results stemming from the performed literature review. However, most of the attacks included in this document have been practically proven by their corresponding paper. We analyzed the exemplary wide area IoT part through extensive research in the domain of agriculture, resulting in five IoT specifics for wide area applications (see Section 3.2). This allowed us to investigate the attacks considering domain-specific constraints, for example, physical access-based attacks are a greater threat for wide area applications than any other IoT domain, and to provide domain-specific recommendations when possible. Since our work is of theoretical nature, a practical analysis should follow in the future.

7 | CONCLUSION

This work inspects the state of security of the communication technology LoRaWAN, that is especially useful for wide area IoT applications, for example, smart agriculture. After giving a short summary into LoRaWAN details, we compile some properties of wide area IoT applications from a security perspective. Especially unsupervised end devices increase the possible attack surface a lot. As the main contribution, we investigated on the research questions, (1) “What are the known vulnerabilities of LoRaWAN?” and (2) “Which mitigations against the known vulnerabilities should be considered when developing a LoRaWAN-based IoT solution?” based on results from a systematic literature review.

This article is intended to help both researchers and developers in the field of wide area IoT due to its completeness and the nature of our provided recommendations. To our knowledge, it is the first work that provides a systematic literature review of LoRaWAN security issues and mitigations. Another unique point of this article is the novel, full list of known LoRaWAN attacks regarding v1.0, v1.1, and backward compatibility mode.

Research has shown that while many LoRaWAN vulnerabilities have been addressed with v1.1, some important issues still remain, for example, RF jamming, physical attacks, and spoofing attacks. With our proposed mitigation options, the risks to be vulnerable to attacks could be reduced.

Future work could include performing a practical evaluation of our findings concerning social responsibility, which are mostly based on theoretical considerations. In this context, we see a deeper investigation of physical attacks and the development of related mitigation strategies to be of prime importance, especially in the domain of agricultural IoT.

ACKNOWLEDGMENTS

This work was supported by funds of the German Government’s Special Purpose Fund held at Landwirtschaftliche Rentenbank in the projects Geobox-II and AgriRegio as well as by the German Federal Ministry for Education and Research (BMBF) in the project HyServ (01IS17030B) and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation)—251805230/GRK 2050. Open access funding enabled and organized by Projekt DEAL.

CONFLICT OF INTEREST

The authors declare no potential conflict of interests.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

ENDNOTE

*https://lora-alliance.org

ORCID

Franz Kuntke https://orcid.org/0000-0002-7656-5919

REFERENCES

1. Rana B, Singh Y, Singh PK. A systematic survey on internet of things: energy efficiency and interoperability perspective. *Trans Emerg Telecommun Technol*. 2021;32(8). doi:10.1002/ett.4166
2. LoRa Alliance. LoRaWAN 1.1 specification; 2017:1-101.
3. Mekki K, Bajic E, Chaxel F, Meyer F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express*. 2019;5(1):1-7. doi:10.1016/j.icte.2017.12.005
4. Yang X, Karampatzakis E, Doerr C, Kuipers F. Security vulnerabilities in LoRaWAN. Proceedings of the IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI); 2018:129-140; IEEE. doi:10.1109/IoTDI.2018.00022
5. Butun I, Pereira N, Gidlund M. Analysis of LoRaWAN v1.1 security: research paper. Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects. Association for Computing Machinery; 2018; New York, NY.
6. Cambra C, Sendra S, Lloret J, Garcia L. An IoT service-oriented system for agriculture monitoring. Proceedings of the IEEE International Conference on Communications; 2017. doi:10.1109/ICC.2017.7996640
7. LoRa Alliance Technical Committee. LoRaWAN ® L2 1.0.4 specification (TS001-1.0.4); 2020:1-75.
8. LoRa Alliance. LoRaWAN 1.0.3 specification; 2018:1-72.
9. Berni AJ, Gregg WD. On the utility of chirp modulation for digital signaling. *IEEE Trans Commun*. 1973;21(6):748-751. doi:10.1109/TCOM.1973.1091721
10. Khutsoane O, Isong B, Abu-Mahfouz AM. IoT devices and applications based on LoRa/LoRaWAN. Proceedings of the IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society 2017; 2017:6107-6112; IEEE. doi:10.1109/IECON.2017.8217061
11. Kuntke F, Sinn M, Reuter C. Reliable data transmission using low power wide area networks (LPWAN) for agricultural applications. Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES). Association for Computing Machinery; 2021; New York, NY.
12. Baumgärtner L, Lieser P, Zobel J, Bloessl B, Steinmetz R, Mezini M. LoRAgent: a DTN-based location-aware communication system using LoRa. Proceedings of the 2020 IEEE Global Humanitarian Technology Conference (GHTC); 2020:1-8.
13. Aras E, Small N, Ramachandran GS, Delbruel S, Joosen W, Hughes D. Selective jamming of LoRaWAN using commodity hardware. Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous 2017). Association for Computing Machinery; 2017:363-372; New York, NY.
14. Dönmez TC, Nigussie E. Security of LoRaWAN v1.1 in backward compatibility scenarios. *Proc Comput Sci*. 2018;134:51-58. doi:10.1016/j.procs.2018.07.143
15. Sontowski S, Gupta M, Laya Chukkapalli SS, et al. Cyber Attacks on Smart Farming Infrastructure; 2020:135-143.
16. Gupta M, Abdelsalam M, Khorsandroo S, Mittal S. Security and privacy in smart farming: challenges and opportunities. *IEEE Access*. 2020;8:34564-34584. doi:10.1109/ACCESS.2020.2975142
17. Demestichas K, Peppes N, Alexakis T. Survey on security threats in agricultural IoT and smart farming. *Sensors*. 2020;20(22). doi:10.3390/s20226458
18. Davcev D, Mitreski K, Trajkovic S, Nikolovski V, Koteli N. IoT agriculture system based on LoRaWAN. Proceedings of the IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS 2018; 2018:1-4. doi:10.1109/WFCS.2018.8402368
19. Grunwald A, Schaarschmidt M, Westerkamp C. LoRaWAN in a rural context: use cases and opportunities for agricultural businesses. Proceedings of the 24 ITG-Symposium on Mobile Communication - Technologies and Applications; 2020:134-139.
20. American heritage dictionary of the English language agriculture; 2021. Accessed February 04, 2021. https://www.ahdictionary.com/word/search.html?q=agriculture
21. Elijah O, Rahman TA, Orikumhi I, Leow CY, Hindia MN. An overview of Internet of Things (IoT) and data analytics in agriculture: benefits and challenges. *IEEE IoT J*. 2018;5(5):3758-3773. doi:10.1109/JIOT.2018.2844296
22. Tzounis A, Katsoulas N, Bartzanas T, Kittas C. Internet of Things in agriculture, recent advances and future challenges. *Biosyst Eng*. 2017;164:31-48. doi:10.1016/j.biosystemseng.2017.09.007
23. West J. A prediction model framework for cyber-attacks to precision agriculture technologies. *J Agric Food Inf*. 2018;19(4):307-330. doi:10.1080/10496505.2017.1417859
24. Geil A, Sagers G, Spaulding AD, Wolf JR. Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry. *Int Food Agribusiness Manag Rev*. 2018;21(3):317-334. doi:10.22434/IFAMR2017.0045
25. Bokusheva R, Kimura S. Cross-country comparison of farm size distribution. *OECD Food, Agric Fisher Pap*. 2016;94:1-46. doi:10.1787/5jlv81sclr35-en
26. Popescu A, Alecu IN, Dinu TA, Stoian E, Condei R, Ciocan H. Farm structure and land concentration in Romania and the European Union's agriculture. *Agric Agric Sci Proc*. 2016;10:566-577. doi:10.1016/j.aaspro.2016.09.036
27. Nikander J, Manninen O, Laajalahti M. Requirements for cybersecurity in agricultural communication networks. *Comput Electron Agric*. 2020;179(October):105776. doi:10.1016/j.compag.2020.105776
28. Hamami L, Nassereddine B. Application of wireless sensor networks in the field of irrigation: a review. *Comput Electron Agric*. 2020;179(April):105782. doi:10.1016/j.compag.2020.105782
29. Terence S, Purushothaman G. Systematic review of Internet of Things in smart farming. *Trans Emerg Telecommun Technol*. 2020;31(6). doi:10.1002/ett.3958
30. Sanjeevi P, Prasanna S, Siva Kumar B, Gunasekaran G, Alagiri I, Vijay AR. Precision agriculture and farming using Internet of Things based on wireless sensor network. *Trans Emerg Telecommun Technol*. 2020;31(12). doi:10.1002/ett.3978

31. Linsner S, Kuntke F, Schmidbauer-Wolf GM, Reuter C. >Blockchain in agriculture 4.0 - an empirical study on farmers expectations towards distributed services based on distributed ledger technology. *Proceedings of Mensch und Computer (MuC)*. Association for Computing Machinery: New York, NY; 2019:103-113.
32. Petit C, Bressoud F, Aubry C. The effects of transition towards short supply chains on liveability of farming systems: initial findings and further research needs. Proceedings of the 9 European IFSA Symposium; 2010:1138-1147.
33. Linsner S, Kuntke F, Steinbrink E, Franken J, Reuter C. The role of privacy in digitalization – analyzing perspectives of German farmers. *Proc Privacy Enhancing Technol*. 2021;2021(3):334-350. doi:10.2478/popets-2021-0050
34. Barreto L, Amaral A. Smart farming: cyber security challenges. Proceedings of the 2018 International Conference on Intelligent Systems (IS); 2018:870-876; IEEE.
35. Rocchetto M, Tippenhauer NO. On attacker models and profiles for cyber-physical systems. *Computer Security – ESORICS 2016*. Cham, Switzerland: Springer International Publishing; 2016:427-449.
36. van Brocke J, Simons A, Riemer K, Niehaves B, Plattfaut R, Cleven A. Standing on the shoulders of giants: challenges and recommendations of literature search in information systems research. *Commun Assoc Inf Syst*. 2015;37. doi:10.17705/1CAIS.03709
37. Kitchenham B, Charters S. Guidelines for performing systematic literature reviews in software engineering. Technical report EBSE-2007-01. Keele University and University of Durham; 2007.
38. Lee J, Hwang D, Park J, Kim KH. Risk analysis and countermeasure for bit-flipping attack in LoRaWAN. Proceedings of the 2017 International Conference on Information Networking (ICOIN); 2017:549-551.
39. Na S, Hwang D, Shin W, Kim KH. Scenario and countermeasure for replay attack using join request messages in LoRaWAN. Proceedings of the 2017 International Conference on Information Networking (ICOIN); 2017:718-720.
40. Aras E, Ramachandran GS, Lawrence P, Hughes D. Exploring the security vulnerabilities of LoRa. Proceedings of the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF); 2017:1-6.
41. Tomasin S, Zulian S, Vangelista L. Security analysis of LoRaWAN join procedure for Internet of Things networks. Proceedings of the 2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW); 2017:1-6.
42. Kim J, Song J. A simple and efficient replay attack prevention scheme for LoRaWAN. Proceedings of the ICCNS 2017. Association for Computing Machinery; 2017:32-36; New York, NY.
43. Gladisch A, Rietschel S, Mundt T, Bauer J, Goltz J, Wiedenmann S. Securely connecting IoT devices with LoRaWAN. Proceedings of the 2018 2nd World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4); 2018:220-229.
44. Sung WJ, Ahn HG, Kim JB, Choi SG. Protecting end-device from replay attack on LoRaWAN. Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT); 2018:167-171.
45. Danish SM, Nasir A, Qureshi HK, Ashfaq AB, Mumtaz S, Rodriguez J. Network intrusion detection system for jamming attack in LoRaWAN join procedure. Proceedings of the 2018 IEEE International Conference on Communications (ICC); 2018:1-6.
46. Benkahla N, Belgacem B, Frikha M. Security analysis in enhanced LoRaWAN duty cycle. Proceedings of the 2018 7th International Conference on Communications and Networking (ComNet); 2018:1-7; IEEE.
47. Skorpil V, Oujezsky V, Palenik L. Internet of Things Security Overview and Practical Demonstration. Proceedings of the 2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT); 2018: 1–7.
48. Cheng Y, Saputra H, Goh LM, Wu Y. Secure smart metering based on LoRa technology. Proceedings of the 2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA); 2018:1-8.
49. Mundt T, Gladisch A, Rietschel S, Bauer J, Goltz J, Wiedenmann S. General security considerations of LoRaWAN version 1.1 infrastructures. Proceedings of the 16th ACM International Symposium on Mobility Management and Wireless Access (MobiWac). Association for Computing Machinery; 2018:118-123; New York, NY.
50. Van Es E, Vranken H, Hommersom A. Denial-of-service attacks on LoRaWAN. Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES). Association for Computing Machinery; 2018; New York, NY.
51. Ruotsalainen H, Grebeniuk S. Towards wireless secret key agreement with LoRa Physical Layer. Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES). Association for Computing Machinery; 2018; New York, NY.
52. Coman FL, Malarski KM, Petersen MN, Ruepp S. Security issues in internet of things: vulnerability analysis of LoRaWAN, Sigfox and NB-IoT. Proceedings of the 2019 Global IoT Summit (GIoTS); 2019:1-6.
53. Wadatkar PV, Chaudhari BS, Zennaro M. Impact of interference on LoRaWAN link performance. Proceedings of the 2019 5th International Conference on Computing, Communication, Control and Automation (ICCUBEA); 2019:1-5.
54. Raad N, Hasan T, Chalak A, Waleed J. Secure data in LoRaWAN network by adaptive method of elliptic-curve cryptography. Proceedings of the 2019 International Conference on Computing and Information Science and Technology and Their Applications (ICCISTA); 2019:1-6.
55. Xu J, Tang Y, Wang Y, Wang X. A practical side-channel attack of a LoRaWAN module using deep learning. Proceedings of the 2019 IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID); 2019:17-21.
56. Hill K, Gagneja KK, Singh N. LoRa PHY range tests and software decoding - physical layer security. Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN); 2019:805-810.
57. Saxena S, Pandey A, Kumar S. A multistage RSSI-based scheme for node compromise detection in IoT networks. Proceedings of the 2019 IEEE 16th India Council International Conference (INDICON); 2019:1-4.
58. Kamble P, Gawade A. Digitalization of healthcare with IoT and cryptographic encryption against DOS attacks. Proceedings of the 2019 International Conference on contemporary Computing and Informatics (IC3I); 2019:69-73.
59. Eldefrawy M, Butun I, Pereira N, Gidlund M. Formal security analysis of LoRaWAN. *Comput Netw*. 2019;148:328-339. doi:10.1016/j.comnet.2018.11.017

60. Mikhaylov K, Fujdiak R, Pouttu A, Miroslav V, Malina L, Mlynek P. Energy attack in LoRaWAN: experimental validation. Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES). Association for Computing Machinery; 2019; New York, NY.
61. Bala S, Barthel D, Gharout S. Separate session key generation approach for network and application flows in LoRaWAN. Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing (SAC); 2019:870-879; Association for Computing Machinery, New York, NY.
62. Thomas J, Cherian S, Chandran S, Pavithran V. Man in the middle attack mitigation in LoRaWAN. Proceedings of the 2020 International Conference on Inventive Computation Technologies (ICICT); 2020:353-358.
63. Philip SJ, McQuillan JM, Adegbite O. LoRaWAN v1.1 security: are we in the clear yet? Proceedings of the 2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application (DependSys); 2020:112-118.
64. Gu C, Jiang L, Tan R, Li M, Huang J. Attack-aware data timestamping in low-power synchronization-free LoRaWAN. Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS); 2020:100-110.
65. Perković T, Siriščević D. Low-Cost LoRaWAN Jammer. Proceedings of the 2020 5th International Conference on Smart and Sustainable Technologies (SpliTech); 2020:1-6.
66. Singh RK, Berkvens R, Weyn M. Synchronization and efficient channel hopping for power efficiency in LoRa networks: a comprehensive study. *Internet of Things*. 2020;11:100233. doi:10.1016/j.iot.2020.100233
67. Noura H, Hatoum T, Salman O, Yaacoub JP, Chehab A. LoRaWAN security survey: issues, threats and possible mitigation techniques. *Internet of Things*. 2020;12:100303. doi:10.1016/j.iot.2020.100303
68. Hessel F, Almon L, Álvarez F. ChirpOTLE: a framework for practical LoRaWAN security evaluation. Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec); 2020:306-316; Association for Computing Machinery, New York, NY.
69. Wang X, Kong L, Wu Z, Cheng L, Xu C, Chen G. SLoRa: towards secure LoRa communications with fine-grained physical layer features. Proceedings of the 18th Conference on Embedded Networked Sensor Systems (SenSys). Association for Computing Machinery; 2020:258-270; New York, NY.
70. Lv Z, Qiao L, Kumar Singh A, Wang Q. AI-empowered IoT security for smart cities. *ACM Trans Internet Technol*. 2021;21(4). doi:10.1145/3406115
71. FIRST. Forum of incident response and security teams . CVSS version 31 specification document; 2019.
72. Butun I, Pereira N, Gidlund M. Security risk analysis of LoRaWAN and future directions. *Future Internet*. 2018;11(1):1-22. doi:10.3390/fi11010003
73. Yang X. *LoRaWAN: Vulnerability Analysis and Practical Exploitation* [M.Sc. thesis]. Delft University of Technology; 2017.
74. Danish SM, Lestas M, Qureshi HK, Zhang K, Asif W, Rajarajan M. Securing the LoRaWAN join procedure using blockchains. *Clust Comput*. 2020;8. doi:10.1007/s10586-020-03064-8
75. Martinez I, Tanguy P, Nouvel F. On the performance evaluation of LoRaWAN under jamming. Proceedings of the 12th IFIP Wireless and Mobile Networking Conference (WMNC); 2019:141-145; IEEE
76. Chacko S, Job MD. Security mechanisms and vulnerabilities in LPWAN. *IOP Conf Ser Mater Sci Eng*. 2018;396:012027. doi:10.1088/1757-899X/396/1/012027

How to cite this article: Kuntke F, Romanenko V, Linsner S, Steinbrink E, Reuter C. LoRaWAN security issues and mitigation options by the example of agricultural IoT scenarios. *Trans Emerging Tel Tech*. 2022;e4452. doi: 10.1002/ett.4452