Field Survey of Wireless M-Bus Encryption for Energy Metering Applications in Residential Buildings

FRIEDRICH HILLER V. GAERTRINGEN, JOHANNES GALENZOWSKI, KAIBIN BAO, SIMON WACZOWICZ, and VEIT HAGENMEYER, Karlsruhe Institute of Technology (KIT), Germany

The wireless Metering-Bus (M-Bus) is widely used in Germany to transmit meter data for heat cost allocation as well as cold and warm water consumption in multi-family apartment buildings. This metering data poses significant privacy risks as it can reveal inhabitants' behaviors. Consequently, the German Heating Cost Ordinance demands this transmission to be both interoperable and secure. However, the wireless M-Bus standard EN 13757 specifies security features as optional. In our work, we conducted a field study by recording sensor telegrams in four cities to assess the implementation of these security features. We analyzed the presence of encryption and the types of metering applications in use. Our findings reveal that about 48.5 % of the recorded sensor devices did not have encryption enabled. Additionally, the use of encryption was found to correlate with specific manufacturers, indicating a systematic acceptance of privacy risks. To demonstrate the impact of unencrypted wireless M-Bus radio telegrams on the privacy, we recorded a wireless M-Bus based warm water meter over a period of several weeks and show that inhabitants' presence and sleep cycles can be inferred from the recordings. These findings underscore the need for mandatory security features in the operation of wireless M-Bus based metering applications to protect consumer privacy.

CCS Concepts: • **Security and privacy** → **Mobile and wireless security**; **Social aspects of security and privacy**; • **Hardware** → *Energy metering*; • **Networks** → Transport protocols.

Additional Key Words and Phrases: Wireless M-Bus, Encryption, Privacy, Field Survey, Cybersecurity, Submetering

Availability of data:
The pseudonymized and processed data of this field study is available online at https://doi.org/10.5281/zenodo.13234545.

1 INTRODUCTION

The German Heating Cost Ordinance (HeizkostenV), amended in 2021, demands the mandatory usage of remotely readable heat cost allocators and warm water meters in buildings in Germany (§ 5 Section 2 of HeizkostenV [7]). The implementation of this ordinance is associated with the obligation to use an interoperable communication standard. In Germany, wireless M-Bus (wM-Bus) is used for this application (Section 3.3.5.2.1 of the BSI-TR-03109-1 [6]). The wM-Bus protocol utilizes frequencies in the ISM band (Industrial, Scientific and Medical Band), as described in EN 13757-4.

For our explorative study, we analyzed broadcasting communication modes. In these modes, each sensor data concentrator records every received radio telegram, and then backend processing later determines which records are used. Following the standard EN 13757, the metering data in the payload of the telegrams can be encrypted to ensure confidentiality. This should ensure that only the metering operator can decrypt the metering data.

As mentioned, the widespread application of wM-Bus is to be expected due to legal requirements. Yet, we identified that statistics about the usage of wM-Bus in the field are not reflected in scientific literature. We saw a need to conduct a field study on how wM-Bus is used in practice. This study also investigates whether there are any obvious security risks to the privacy of residents due to the operation of these continuously transmitting devices.

Consequently, in our work, we target the following research questions:

RQ1 Which impact on privacy do meters using wireless M-Bus have in practice?
RQ2 Is it possible to capture, interpret and spatially allocate wireless M-Bus telegrams in the field?
RQ3 Are the captured wireless M-Bus telegrams protected by encryption or other security measures?
RQ4 Do the unprotected telegrams or unprotected telegram parts expose sensitive data?

The remainder of the paper is structured in the following way: We investigate at the related literature in Section 2. In Section 3, we present the most relevant parts of the wM-Bus standard which we used to conduct the field study and data analysis. The design of the device to capture and spatially allocate wM-Bus telegrams is described in Section 4. Subsequently, we present the results of our field study in Section 5, including statistics of used encryption, device types and a demonstration of the impact on privacy. In Section 6, we discuss the limitations of our field study. Finally, we describe the responsible disclosure process of our findings in Section 7 and conclude our study in Section 8.

2 RELATED WORK ON WIRELESS M-BUS SECURITY

Most related literature focuses on the advancement of the functional aspect of wM-Bus. This includes the work of Squartini et al., who explore wM-Bus in the context of smart water grid applications, focusing on energy consumption and efficiency [17]. The work of Spinsante et al. [15, 16] investigates the suitability and efficiency of the wM-Bus protocol for smart water grids. Spinsante et al. highlight the wM-Bus protocol's potential in automatic monitoring and smart metering of water consumption with an energy-efficient network architecture. Pavel Masek et al. [9, 10] demonstrate the potential of wM-Bus protocol for smart electricity grids and 5G-grade home automation.

Another line of research focuses on the privacy issues associated with smart metering. Lisovich et al. [8] demonstrate the possibility to infer which movies inhabitants watch based on a time series of the household's electricity consumption. Chen et al. [5] propose a statistical framework for disaggregating utility consumption from smart meters with low sample rates into specific appliance usage associated with human activities. Asghar et al. [2] review the uses

Authors' address: Friedrich Hiller v. Gaertringen, friedrich.gaertringen9@kit.edu; Johannes Galenzowski, johannes.galenzowski@kit.edu; Kaibin Bao, kaibin.bao@kit.edu; Simon Waczowicz, simon.waczowicz@kit.edu; Veit Hagenmeyer, veit.hagenmeyer@kit.edu, Karlsruhe Institute of Technology (KIT), Kaiserstr. 12, 76131, Karlsruhe, Germany.

of metering data in the smart grid and related privacy legislation. They provide a structured overview of security solutions for privacy-preserving meter data delivery and management. Moreover, they survey recent work on privacy-preserving technologies for billing, operations, and value-added services including demand response. As a key result, they identify the need for metering solutions that balance privacy concerns with the functionality of smart metering systems.

Researchers also propose extensions of the wM-Bus protocol for enhanced security. Anani and Ouda [1] propose a security framework for wM-Bus within the smart grid communication network, introducing a new lightweight security profile with less impact on battery life.

A limited number of publications perform a security analysis and expose shortcomings of the protocol or issues of the real-world implementations of wM-Bus. Polčák and Matoušek [12] highlight a concern with wM-Bus meters that monitor energy consumption at short intervals, such as every minute, increasing privacy and security risks. In their case-study, they investigated devices from two wM-Bus vendors and found four CVE[1]-indexed security vulnerabilities:

Broken Key Management The authors demonstrated that metering data acquisition devices of a manufacturer could receive meter data without specifying the encryption key. Either a shared key is used across all devices, or the key can be derived using the serial number.

Zero Consumption Detection Even though the payload of the wM-Bus telegrams are encrypted, it is still distinguishable whether the metering values change between transmissions.

Vulnerability to Replay Attacks The readout software does not adequately detect the replay of previously recorded telegrams.

Misleading Event Detection The readout software showed misleading events related to tampering detection.

Additionally, a white paper by Brunschwiler [4] presents a detailed security analysis of the wM-Bus standard. Several vulnerabilities were found in this paper, including:

Inadequate Key Length The standard suggests that only half of the key length shall be different for each meter, reducing the key strength significantly.

Zero Consumption Detection Inappropriate key and initialization vector use allows inferring unchanged meter counter values, indicating zero consumption detection.

Consumption Values Inappropriate key and initialization vector derivation may disclose plain texts including consumption values.

Manipulation of encrypted telegrams Missing integrity protection allows for manipulation of consumption values in transit.

Clock synchronization Lack of authentication with clock updates may lead to key stream repetition.

Network Management Lack of authentication for network management could allow adversaries to become a rogue relay.

Unencrypted tamper detection Plain text error and alarm notifications allow an adversary to recognize if tamper switches have been triggered.

Unencrypted identification Unencrypted disclosure of device manufacturer, meter type and version ID in the device's telegrams simplify identification of vulnerable targets.

Key Management Loosely specified key update mechanism may lead to key disclosure. Some transceiver chips support the transparent decoding of encrypted telegrams. The encryption key is not protected and can be read out.

Finally, there are open-source implementations to transceive or decode wM-Bus radio telegrams. For example, wmbusmeters[2] is a decoder for wM-Bus telegrams, including some manufacture-specific encodings. Also worth mentioning is the rtl-wmbus[3] library, a Software Defined Radio library for decoding the physical layer of wM-Bus.

All existing works do not include extensive field studies investigating the usage and security of a large number of metering devices in real-world operation. Existing work does not always describe the exact number of investigated metering devices in total. But where numbers are given, either the number of metering device models or the number of individual metering devices were below 20. By recording wM-Bus signals in the field, we expect to capture at least several hundred individual metering devices.

Our field study targets the research gap regarding real-world usage and draws inspiration from Peter Shiple's concept of War-Driving presented at the DEF CON 9 conference [14]. War-Driving describes the process of mapping Wi-Fi networks by logging Wi-Fi Access Point beacons and correlating it with a location gathered using a Global Navigation Satellite System. In a non-representative initial study dating back to the year 2000, Shiple located around 1500 Access Points from which 85% were not using encryption [14]. Ten years later, Said et al. scanned 1228 Access Points in Dubai from which 35% were not encrypted and 26% used weak encryption [13].

3 WIRELESS M-BUS TELEGRAM PROCESSING BASED ON THE EN 13757 STANDARD

This chapter aims to explain all the technical principles necessary for analyzing the wM-Bus data collected in our field study. As the EN 13757 wM-Bus standard comprises eight parts and over 750 pages, this section cannot provide a comprehensive breakdown. Rather, it specifically isolates and describes the knowledge that is essential for our use case. It for the proposed research questions, it is essential, to differentiate whether an individual sensor uses encryption, of what device type it is, and from which manufacturer it originates. Additionally, this chapter describes how sensor data of unencrypted wM-Bus telegrams are decoded to access the impact on privacy.

[1] Common Vulnerability Enumeration, https://cve.mitre.org/

[2] https://github.com/wmbusmeters/wmbusmeters

[3] https://github.com/xaelsouth/rtl-wmbus

3.1 History and overview of EN 13757

The Metering-Bus (M-Bus) was originally developed by Horst Ziegler in 1992 [3]. Originally, DIN EN 1434 proposed the M-Bus protocol for the metering of heat energy consumption. Later, M-Bus is described as a separate standard set DIN EN 13757. Following the European Union Directive 2006/32/EG, which set the goal to save final energy consumption through optimizing energy-related services and other energy efficiency measures by 9%, a new means for measuring energy consumption was required. The Open Metering System (OMS) was developed to address the metering of energy consumption and proposed a technical solution based on the M-Bus protocol.

At the time of publication of the present paper, the European standard EN 13757 specifies all aspects of the (wireless) M-Bus protocol, from the physical layers up to the application layer. The EN 13757 standard is divided into eight parts, as shown in Table 1.

Table 1. Overview of the eight parts of the M-Bus standard EN 13757.

Part Nr.	Brief Description
EN 13757-1	General overview of the data exchange and communication, as well as the protocol, used on different layers for remote reading of metering values.
EN 13757-2	Physical and data link layer of the *wired* M-Bus protocol.
EN 13757-3	Application layer of the meter bus protocol, which is independent of the physical transmission medium.
EN 13757-4	Physical and data link layer of the *wireless* M-Bus protocol.
EN 13757-5	Retransmission, relaying and routing for the wireless protocol.
EN 13757-6	Description of a wired local bus for meter readings over short distance as an alternative to the M-Bus specified in part two.
EN 13757-7	Definition of the session and transport layers, including transport layer encryption.
EN 13757-8	Extension to usability of M-Bus in wireless communication outside the standard of part four.

In the following subsections, we will briefly outline which of these parts are particularly relevant and structure their content to enable the extraction of the relevant information from the wM-Bus telegrams.

3.2 OSI-layer-wise description of M-Bus telegrams

We obtain a structured overview by mapping each part of EN 13757 to the layers of the OSI reference model in Table 2. This allows a dedicated analysis of the different sections of a M-Bus telegrams.

Starting from the physical layer at the bottom of Table 2, the first distinction is between wired and wireless M-Bus. Parts two and six of the standard cover the wired part and can therefore be discarded for a field study focussing on wireless drive-by readout. Since in the case of meters, there is only the sending device and no forwarding via gateways, routed transmission as described in EN 13757-5 is also disregarded. Therefore, only EN 13757-4 is the decisive standard for analyzing the physical layer in the context of our study (see Section 3.2.1).

The parts of EN 13757 relevant for layer 2 to 7 are also depicted in Table 2. Our particular interest in encryption requires a more in-depth analysis of the layers 2 (13757-2 and 13757-4) and 4 (13757-7). Furthermore, to analyze whether privacy-relevant data can be extracted, it is necessary to look at the application layer (EN 13757-3). To summarize, we need an analysis of the standard parts 2, 3, 4, 5, and 7.

Table 2. OSI layers of M-Bus and related standard parts (based on EN 13757-1 Table 3 and EN 13757-7 Table 1).

OSI layer		Wired M-Bus	Wireless M-Bus
7	Application Layer	EN 13757-3	
6 5 4	Presentation Layer Session Layer Transport Layer	optional, depending on CI-Field (EN 13757-7)	
3	Network Layer	optional, depending on CI-Field (EN 13757-5)	
2	Data Link Layer	EN 13757-2 / extended by EN 13757-4 / based on IEC 60870-5	
1	Physical Layer	wired M-Bus (EN 13757-2) wired local bus (EN 13757-6)	direct transmission (EN 13757-4) routed transmission (EN 13757-5)

3.2.1 *Physical Layer (EN 13757-4).*

An understanding of the physical layer is primarily relevant for designing a suitable data acquisition device. The physical layer of wM-Bus can be operated in different modes that are optimized towards specific use cases. Mode S is used for communication among stationary devices. Mode F and N are used for longer distances. Mode C and T are optimized towards drive-by readouts.

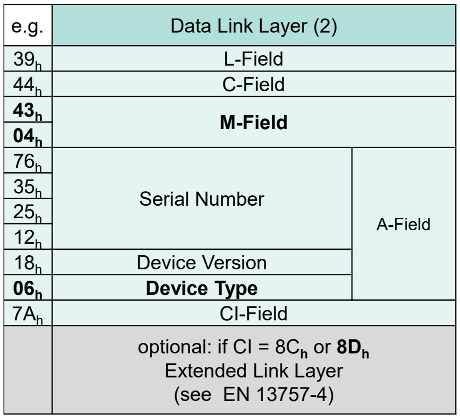
The radio frequencies and symbol rates of each mode are different, such that a transceiver usually needs to be set to a specific mode. However, the frequency and symbol rate of mode C and T used for the channel from the sensor to the collector is equivalent. That is, the receiver can receive both C and T telegrams if tuned to the same frequency and symbol rate. Despite this, the encoding schemes are different. The byte rate also differs due to the encoding scheme. However, using a separate decoding scheme for each mode, C and T mode can be received in parallel.

The modes are further divided into sub-modes to distinguish between unidirectional communication (designated as S1, C1, etc.) and bidirectional communication (designated as S2, C2, etc.).

In our work, we only analyze sensor telegrams received by passively listening. We do not request the sensors for readouts and rely on unsolicited frequent transmissions. This field study therefore only considers mode C1 and T1.

3.2.2 *Data Link Layer (EN 13757-2 and EN 13757-4).*

The data link layer consists of a header containing the length of the telegram, manufacturer and serial number, as well as the device type and telegram type contained in the telegram (see Figure 1). Another part of the data link layer is the trailer field, which contains a checksum for cyclic redundancy check (CRC). Since integrity checking is commonly integrated in the receiving device, the CRC is relevant when selecting a suitable data acquisition device, but is not required



e.g.	Data Link Layer (2)	
39_h	L-Field	
44_h	C-Field	
43_h	**M-Field**	
04_h		
76_h	Serial Number	A-Field
35_h		
25_h		
12_h		
18_h	Device Version	
06_h	**Device Type**	
$7A_h$	CI-Field	
	optional: if CI = $8C_h$ or **$8D_h$** Extended Link Layer (see EN 13757-4)	

Fig. 1. Example of a data link layer of one of our captured telegrams. In **bold** the fields included in our statistical evaluation. For the overview of a full telegram, see Figure 12.

to be analyzed for our research questions. It is important to note that the header fields of the data link layer is always unencrypted, which always allows the identification of the sending device. All the header fields required for our analysis are briefly explained below.

L- and C-Field. The one byte long L-Field states of how many bytes the telegram consists of (for example, 39_h indicates a telegram with 57 bytes). The subsequent one byte long C-Field describes the sending mode. As described in Section 3.2.1 we captured communication mode C1/T1. With only listening to one-directional openly broadcasted telegrams, we only captured C-Fields with 44_h corresponding to "SEND/NO REPLY, Meter initiative" according to EN 13757-4. These two fields are neither statistically evaluated nor technically required for further evaluation.

M-Field. The first field of the header that we evaluated statistically is the M-Field. The M-Field contains the manufacturer ID, which is assigned by the DLMS User Association and encoded according to EN 13757-7 7.5.2 in the form of three letters coded in two bytes. We evaluate the M-Field to be able to analyze differences in encryption usage between manufacturers.

A-Field. The A-Field serves two purposes. Firstly, it allows the device to be unambiguously identified. This is possible through the unique combination of the four byte serial number and the one byte device version. This part of the A-Field not statistically evaluated, but is technically required to identify and group several telegrams from the same device. Secondly, the A-Field contains one byte specifying the device type. The device type field was evaluated according to EN 13757-7 Table 13.

CI-Field. The most important field for subsequent decoding is the CI-Field. For all layers above the data link layer, CI-Fields are used to specify what the next telegram segment looks like. For our evaluation, it is relevant to be able to understand the following multiple numbers of telegram sequences so far, until the segment concerning encryption or interpretable user data is encountered and can be evaluated. The segment containing the relevant information may already be defined in the CI-Field found on the data link layer, but may also be encoded in the subsequent telegram segment on the transport layer or the application layer. In those cases, further CI-Fields are present on the data link layer. In any case, the CI-Fields must be evaluated segment by segment to be able to analyze the subsequent data.

The lowest level at which an insight can be gained is in the data link layer in the case of a CI-Field of $8D_h$. A CI-Field of $8D_h$ indicates that the telegram is encrypted at the data link layer. We can therefore count these telegrams as "encrypted at the data link layer" meaning no further evaluation of their content is done.

In the case of all other CI-Fields we encountered, it is necessary to decode also the next higher (transport) layer, according to the CI-Field defined in the header of the data link layer. In the simplest case, those CI-Fields are CI = 78_h (no header), CI = 72_h (short header) and CI = $7A_h$ or $7B_h$ (long header).

In a more complex case, we find some further sequences between the initial CI-Field of the header and the CI-Field of interest (also 78_h, 72_h, $7A_h$or $7B_h$). This is the case when an extended link layer exists, that is not encrypted (CI = $8C_h$) and we find a further sequence on the transport layer (CI = 90_h), the so-called Authentication and Fragmentation Layer (AFL). Only after those two sequences, we then find the CI-Field of interest for further analysis.

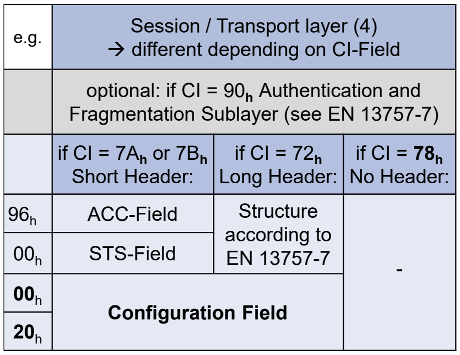
Data Link Layer Encryption (EN 13757-4). Taking a further look at the encryption, we observed that the majority of encryption is applied at the transport layer (see Section 3.2.3). In our data set, only a total of 18 telegrams were encrypted at the data link layer, indicated by a CI-Field of $8D_h$. The used encryption scheme for the data link layer encryption (DLL encryption) is AES-128 in Counter Mode (CTR). The Initial Vector consists of a relative timestamp, a session counter and a block counter. The telegram payload does not need to be padded, as the CTR mode produces a cipher stream that can be truncated at any position.

3.2.3 *Transport Layer (EN 13757-7).*

After deriving possible CI values of 78_h, 72_h, $7A_h$ or $7B_h$, in the following, we discuss, how subsequent telegram sequences can be analyzed on the transport layer (also see Figure 2). For this, we have to differentiate the case for each individual CI value. Telegrams with no header on the transport layer (CI = 78_h) can be classified as not encrypted according to the EN 13757 standard. For those, the next analysis step can continue on the application layer. For the other cases with a short or long header, a Configuration Field exists in the telegram, which is explained in more detail later. In addition to the Configuration Field, other header fields like ACC and STS are present (as shown in Figure 2).

ACC- and STS-Field. The one byte access number in the ACC-Field is counted up when new values are transmitted in a new telegram to indicate that it is not simply a retransmission of the same telegram content. The one byte status field (STS-Field) describes the error state of the device. The STS-Field's bits zero and one (underlined) define the error type:

- 0000 00$\underline{00}_b$= no error
- 0000 00$\underline{01}_b$= application busy
- 0000 00$\underline{10}_b$= arbitrary application error
- $\cdots t\,pe\underline{11}_b$= unusual state/alarm



e.g.	Session / Transport layer (4) → different depending on CI-Field		
	optional: if CI = 90$_h$ Authentication and Fragmentation Sublayer (see EN 13757-7)		
	if CI = 7A$_h$ or 7B$_h$ Short Header:	if CI = 72$_h$ Long Header:	if CI = **78$_h$** No Header:
96$_h$	ACC-Field	Structure according to EN 13757-7	-
00$_h$	STS-Field		
00$_h$	**Configuration Field**		
20$_h$			

Fig. 2. Example of the transport layer of one of our captured telegrams. In **bold** the fields included in our statistical evaluation.

Bits two to seven further specify the error. Bit two (e) is set to one if energy supply is low, bit three (p) is set if a permanent error is present, and bit four (t) is set if a temporary error is present. Bit five's to seven's functions are not standardized, and reserved for manufacturer-specific error codes. The ACC- and STS-Fields are not used in our evaluation.

Configuration Field. The Configuration Field consists of two bytes. It specifies the protection mode (type of encryption), other required bits, further required transport layer fields (header or trailer) and, if present, the Configuration Field extension. It contains information relevant for a security analysis of the wM-Bus telegrams. The information in the Configuration Field is encoded in binary. It needs to be decoded according to Table 3. In particular, we derive information about the encryption from the Configuration Field. The five protection mode bits (bits 8 to 12 as shown in Table 3) can store values from 0 to 31. The security mode is indicated directly by the number calculated from the bits, as described in the following paragraph.

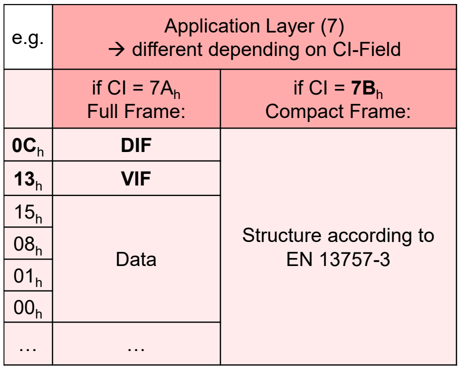
Transport Layer Encryption Modes (EN 13757-7). For security and privacy, wireless M-Bus supports optional encryption modes at the transport layer for the application data. A list of all 16 encryption modes is described in EN 13757-7 (p. 33 Table 19). We observed encryption modes 0, 5, 7 and 10 being used in our field study and therefore describe them more detailed in the following.

- **In mode 0,** the application data is unencrypted.
- **In mode 5,** the application data is encrypted using the symmetric block cypher AES-128 in cipher block chaining (CBC) mode with a static key. The encryption key is static for each metering device. The Initialization vector (IV) is constructed using the manufacturer identifier, the meter identifier, version, device type and access number. All information, from which the IV is calculated, is present in the headers of the telegram.
- **In mode 7,** the used encryption is also the symmetric block cypher AES-128 in cipher block chaining (CBC). But the encryption key is dynamically derived based on a static master key, a use-case-dependent constant, a telegram counter and the sensor id. The freshness of the ciphertext is thus provided by this key derivation instead of using different IVs (in mode 5). Consequently, the IV is not needed to provide security features and is therefore set to zero and not utilized in mode 7. For mode 7, a cypher-based message authentication code (CMAC) is recommended using the authentication and fragmentation sub-layer (AFL).
- **In mode 10,** the 128-bit AES block cypher is used in CCM mode, which is counter mode with CBC-MAC. A 32-bit counter is encrypted using the AES block cypher. The resulting key stream is xored with the plaintext to get the ciphertext. A CBC-MAC is calculated in parallel where the most significant 4, 8, 12, or 16 bytes are appended to the telegram as an authentication tag. The authentication tag size is defined in the extended configuration field of the transport header. The counter is either defined as an optional field of the configuration frame or as a field in the authentication and fragmentation layer (AFL).

Mode 0 does not provide any security guarantees. Mode 5 provides confidentiality only and mode 7 optionally provides integrity and authenticity, if a CMAC is used in conjunction with the AFL. Mode 10 always provides confidentiality, integrity, and authenticity.

3.2.4 *Application Layer (EN 13757-3).*

In cases where either no header is defined on the transport layer (CI = 78$_h$) or encryption mode 0 is defined in the Configuration Field, it must be assumed that the user data is not encrypted in accordance with the EN 13757 standard. In this case, it can be further investigated whether the actual application data can be extracted.



e.g.	Application Layer (7) → different depending on CI-Field	
	if CI = 7A$_h$ Full Frame:	if CI = **7B$_h$** Compact Frame:
0C$_h$	**DIF**	Structure according to EN 13757-3
13$_h$	**VIF**	
15$_h$	Data	
08$_h$		
01$_h$		
00$_h$		
…	…	

Fig. 3. Example of the application layer of one of our captured telegrams. In **bold** the fields included in our statistical evaluation.

Payload structure. Application data is formatted either as a compact frame or a full frame (compare Figure 3). The frame type is determined by the preceding CI-Field. In the compact frame, the metadata and the actual metering data are transmitted in separate telegrams that must be combined for interpretation. This allows a data-saving (compact) transmission of the metering data. However, it also means that pure data telegrams containing a compact frame cannot be interpreted. Further knowledge is required for their evaluation. Full frames, on the other hand, contain the metering and metadata in the same telegram. We therefore use telegrams with a full frame as an example to analyze the received data regarding privacy problems. The structure of a full frame is therefore briefly described below.

Table 3. Decoding of the Configuration Field (CF) according to EN 13757-7 Table 27 (with the least significant bit (LSB) corresponding to bit zero and the most significant bit (MSB) to 15) for an unencrypted telegram example: 00_h20_hresp. 00100000_b,00000000_bin binary (for details see references in table).

Bit number	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Content	Bidirectional communication	Accessibility	Synchronized	Security mode	Security mode	Security mode	Security mode	Security mode	Reserved	Reserved	Reserved	Reserved	Telegram content	Telegram content	Repeater access	Hop counter
Short	B	A	S	M	M	M	M	M	0	0	0	0	C	C	R	H
Reference	EN 13757-7 7.7.1		EN 13757-7 7.7.1	EN 13757-7 Tab 19					0b	0b	0b	0b	EN 13757-7 7.7.1. Tab 21 & 22		EN 13757-5	EN 13757-5
Example	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Description example	no access window (unidirectional meter)		synchronized transmission	no security mode									standard telegram		meters are always zero here	

Full frame. Application data, i.e., sensor values, are arranged in consecutive data records. Each data record starts with a data record header (DRH) describing the data type, encoding, length and metadata of the data record.

The DRH consists of a data information field (DIF) and a value information field (VIF). There are optional data information field extensions (DIFE), value information field extensions (VIFE) and a variable length field (LVAR).

Both standard data types (in the DIF) and standard units (in the VIF) can be used, as well as proprietary codes. The DIF values for standard data types can, for example, be found in Table 4 of EN 13757-3. The VIF values for standard units can be found in Table 10 of EN 13757-3.

In any case, knowledge of the meaning of the DIF and VIF, either from the standard or the manufacturer's documentation, is required for the interpretation of the values contained in the data block. In each of these cases, user data can be accessed and analyzed. More specific, the data information field (DIF) contains two function bits, that indicates if the corresponding value is maximum, minimum, error state or instant value (both bits of the function field are zero).

In our work, if we identify successfully that the telegram contains a full frame (CI = $7A_h$) and the first data block contains an instant value (function bits both zero), we can conclude that this telegram contains real instant metering values. In this case, we consider this telegram as interpreted. Otherwise, the telegrams would be considered as still unencrypted but also as not interpreted by us.

For our example, with a data point with DIF = $0C_h$we know that it is an instant value, Binary Coded Decimal number. With VIF = 13_hwe know, it is a volume in the range 10^{3-6} with the unit m^3. And with the data being $15_h08_h01_h00_h$we know, the value is 10815. We can therefore conclude that the given data represents the current meter value with 10 815 m^3.

With this understanding of EN 13757, the following section describes how the data of our field study were collected and analyzed.

4 DATA ACQUISITION

The goal of the field study was to collect wM-Bus communication samples from as many unique sensor devices as possible. As the sensors are stationary, the data acquisition device must be portable so that it can be transported to multiple locations to capture telegrams of different sensors. The acquisition device therefore is built to be battery-powered and also includes a GPS module to geo-reference each captured telegram. This setup allows a data collection process similar to war-driving to map wireless networks (see Section 2).

We limited our field study to listening to telegrams from continuously sending devices. In this way, our acquisition system does not interfere with the metering system. The setup consists of low-cost commercial off-the-shelf modules and enables undetectable acquisition of metering data from third-party devices.

In preliminary experiments, we noticed that many wM-Bus devices regularly send metering data with an interval between 1 and 15 minutes, which is in line with the observations by Polčák and Matoušek [12].

4.1 Portable Wireless M-Bus Data Acquisition Device

The portable data acquisition device is depicted in Figure 4. The components are referenced in the following using the numbers in the brackets.

The wM-Bus telegrams were captured with a iM871A-USB dongle from IMST GmbH (Figure 4, I). After a firmware update, the iM871A-USB is configured to capture wM-Bus telegrams in combined C1/T1 mode. The CRC-Field is not passed on by the iM871A-USB and only the header and data blocks were recorded. The geolocation was acquired using a GY-GPS6MV2 GPS Module (Figure 4, II) and its antenna (Figure 4, III). A Raspberry Pi Zero W was used as the

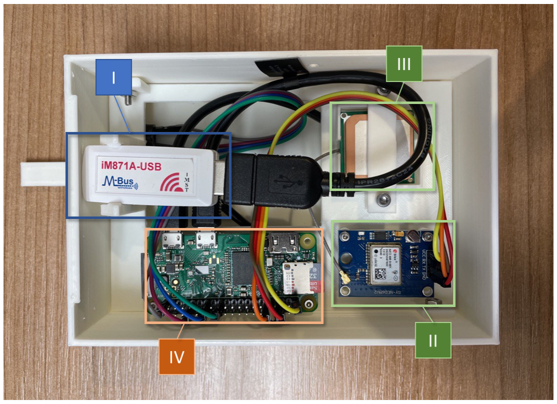


Fig. 4. The main components of our portable wM-Bus data acquisition device, referenced in Section 4.1.

processing and control unit (Figure 4, IV). Additionally, a basic buzzer was used for audible feedback each time a telegram was received. We used a 5 V USB external battery pack with 10 400 mA h to power the device. This battery allowed to operate the acquisition device for more than 24 hours. All components were mounted inside a self-designed 3D-printed enclosure.

4.2 Data Collection Process

The data acquisition device records all received telegrams together with a time stamp and the current geolocation. The recording device itself does not carry out the decoding of the received telegrams. Each of the telegrams is stored in hexadecimal representation with a sequence number, timestamp, and a numerical location identifier in CSV format. The locations are stored separately in JSON format.

The data collection was undertaken in the years 2022 and 2023 by walking through the German cities Munich, Trier, and Karlsruhe, as well as Luxembourg. The majority of data was captured in Munich. We walked along major streets of these cities, starting from multiple randomly selected starting locations. Sometimes, tramlines were used.

Decoding of the telegrams was done later in an iterative process with a proprietary library written by us in Python. The library does not implement the comprehensive wM-Bus standard but was extended incrementally to handle the observed telegrams.

5 RESULTS

In this section, we present the data collected using the data acquisition device presented in Section 4 and the knowledge about decoding derived in Section 3. In Section 5.1, we confirm RQ2 that it is possible to capture, interpret and spatially allocate wM-Bus telegrams from arbitrary sensors in the field. The metering application for which the wM-Bus devices are used and whether manufacturers specialize on specific metering applications is described in Section 5.2. In Section 5.3, we analyze which encryption mode is used by the devices which addresses RQ3, inquiring if wM-Bus telegrams are protected. Finally, Section 5.4 demonstrates how metering data recorded from wM-Bus devices impacts privacy, answering RQ4 that wM-Bus telegrams expose sensitive data. The pseudonymized and processed data of this field study is available online[4].

5.1 Statistics of the Field Study

To answer RQ2, whether it is possible to receive data from arbitrary wM-Bus sensors, we listened to wM-Bus telegrams in the German cities Munich, Trier, and Karlsruhe as well as in Luxembourg using our data acquisition device.

The telegrams were captured during several measuring rounds between 2022-07-22 and 2023-05-21. In total, 13.537 wM-Bus telegrams were recorded. As described in Section 3.2, the unencrypted header allows the unambiguous identification of the device that is sending a given telegram.

Identifying Unique Devices. The 13.537 wM-Bus telegrams could be assigned to 4.986 unique wireless M-Bus devices based on manufacturer ID and serial number.

The distribution of how many telegrams were recorded per device during the entire field study is shown in Figure 5. For about 65 % of the devices, only a single telegram was recorded. For the other 35 % of devices, two or more telegrams were received.

There was no structural difference in the telegrams that we received from the 35 % of devices from which we captured multiple telegrams. In particular, static metadata from the header has remained the same for all telegrams from the same device. Only the user data such as power consumption has changed. For this reason, in the following, we do not analyze the metadata of the header for each telegram, but for each unique device.

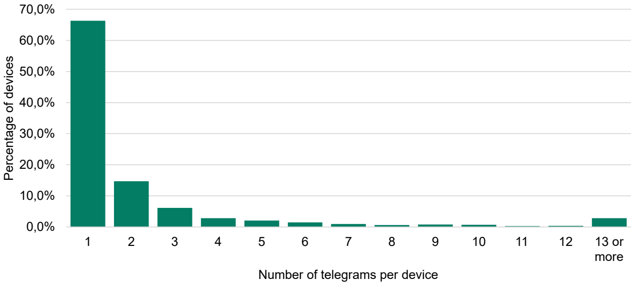


Fig. 5. The percentage of devices over the number of telegrams received from the same device. Only from one third of the devices, more than one telegram was captured during the entire field study.

Distribution of Recorded Devices by Year. The field study was conducted in the years 2022 and 2023, partially repeating the measurement in the same cities. Figure 6 shows how many unique devices were registered in the respective years. Twelve percent of the devices were recorded both in 2022 and 2023. No specific method was used to ensure that the same receiving conditions applied in both years. For example, no effort was made to be in the exact location at the exact time of day or to walk at the exact speed on the same shoulder of the road. If one wanted to compare the years not only

[4] https://doi.org/10.5281/zenodo.13234545

qualitatively, but also quantitatively, a methodically defined walking procedure would be necessary.

If the telegrams had been recorded exactly in the same area, an overlap rate of 84% to 90% would have been expected due to the calibration validity and therefore lifetime of a single meter of six years (according to annex 7 (to § 34 paragraph 1 number 1) of [11]). However, the overlap between the years is lesser, as the data was only partially recorded in the same areas. From the 4.986 devices, 1.485 devices were only captured in 2022, 2.887 only in 2023, and 614 devices in both years (see Figure 6). This corresponds to twelve percent of devices being captured in both years.

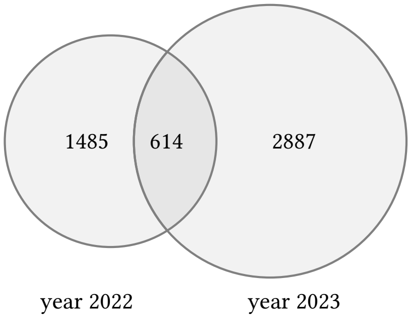


Fig. 6. Observed number of unique devices per year.

Spacial Allocation. Consequently, it can be concluded that it is possible to record a considerable number of third-party devices with moderate effort (compare RQ2). The spatial allocation was not carried out at the apartment level. Rather, the meter's location was roughly determined via an average of the GPS positions, at which the meter's telegrams were received. This results in an accuracy of only several meters. However, other works such as [12] show that a more precise spatial allocation is technically feasible with further effort. Therefore, we can answer RQ2's aspect of spatial allocation, with: yes, it is possible to specially allocate the received telegrams.

Regarding the first general analysis before answering the question about privacy, it remains to be answered which data can be exploited from the telegrams.

5.2 Device Types and Device Manufacturers

As described in Section 3.2, all header information can be decoded in plain text according to the EN 13757 standard. Analyzing this information is used to reveal correlations between encryption modes, device types and device manufacturers. The device type is crucial information to determine the severity and duration of privacy violations. Regarding the severity, cold or warm water meters generate the most sensitive data, heating cost allocator data is medium severe and smoke detector data has the lowest impact on privacy. Regarding the duration, the exchange rate depends on the device type due to calibration period or battery lifespan.

As shown in Fig. 7, the majority of the recorded devices are heat cost allocators. These are followed by hot water meters and water meters (which do not define whether they are used for hot or cold water).

If heat cost allocators are used, they must be installed on every radiator, while heat meters and water meters (cold & hot) are usually only installed at the pipe near the connection point of the accommodation unit or at a maximum on every tap in the apartment. Based on these facts, it is plausible that most of the devices recorded are heat cost allocators. Since consumption-based billing is usually legally obligatory for centralized hot water supply, it is also understandable that hot water meters represent the second-largest group of devices.

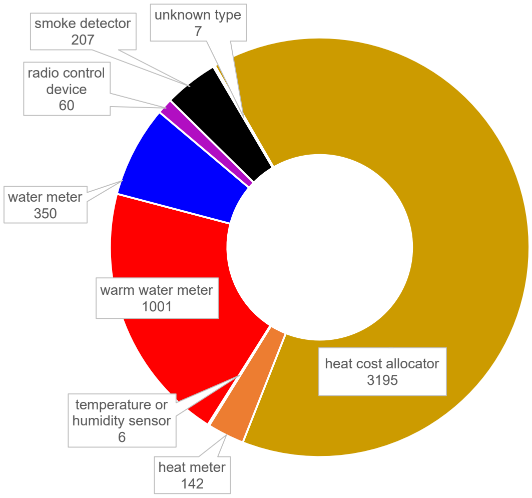


Fig. 7. Device Types. For details, see Section 3 and EN 13757-7 Table 13.

Furthermore, the examined telegrams could be assigned to 15 different manufacturers based on the manufacturer IDs. Thereby, we only consider the manufacturer IDs of the wireless transmitting device. In the case of an attached transmitter module whose manufacturer ID differs from that of the meter, we only consider the manufacturer ID of the transmitter module, as our investigation relates to the radio protocol. The most frequent observed manufacturers are shown in Figure 8. For a detailed description, of how this information can be derived from the M-Field and Device Type field, see Section 3.2.2. In our sample, MAN1 and MAN2 appear to be predominant. MAN3 and MAN4 are still partially widespread, and the other eleven manufacturers only to a minuscule extent. In general, according to our field study, it appears that there are only a few manufacturers who dominate the market.

At this point, all data from the header were evaluated. This header data is required for all telegrams. Although the header data allows conclusions to be drawn about the manufacturer and the devices used, this data does not initially reveal sensitive information. However, the number and the type of appliance recorded in a certain area certainly allow conclusions to be drawn about the structural condition or the heating system used. At first glance, however, no personal data can be generated from this.

For the telegram header, RQ4 can be answered to the extent that the non-encrypted header does not contain any critical information. For a complete response, however, the data block of the telegrams

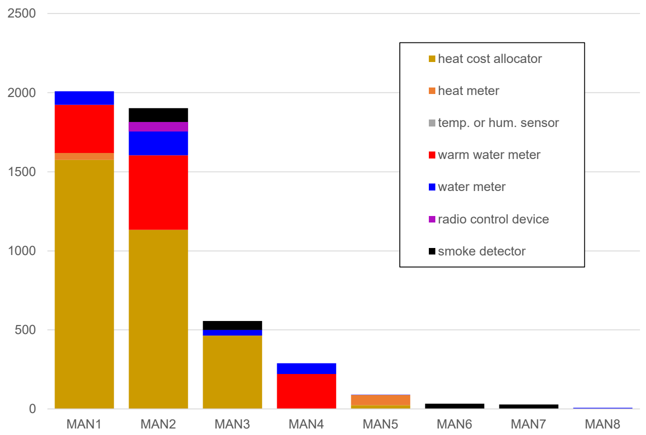


Fig. 8. Number of captured devices and their types ordered by manufacturer identifier (pseudonymized). Manufacturers observed less than five times are not shown (20 devices in total omitted).

must also be considered. The first step is to check whether the data blocks are encrypted to answer RQ3.

5.3 Usage of Encryption

The wM-Bus telegrams are encrypted at the transport layer (see Section 3.2.3) or optionally use the data link layer (DLL) encryption (see Section 3.2.2). In our field study, telegrams with the modes 0, 5, 7, 10 (see Section 3.2.4) as well as DLL (see Section 3.2.2) encryption were observed. The overview of the identified devices separated by the encryption methods is shown in Figure 9. In 2022, 56.6 % of the devices did not use encryption. In 2023, this figure is reduced to 46.7 %. Of the total number of devices recorded over both years, 48.5 % were not encrypted. Among the encrypted devices, mode 5 dominates with around a third of the encrypted devices.

The decoder used for this work has only a basic implementation of the wM-Bus protocol, and therefore cannot decode or interpret the full range of manufacturer-specific modifications to the wM-Bus telegram. For this reason, an additional distinction was made between *interpretable* and *non-interpretable* in the evaluation for mode 0. *Interpretable* are all telegrams for which the first data record could be evaluated according to Section 3.2.4.

The share of encrypted devices seems to have slightly increased in 2023. However, this is not confidentially deductible from the data, due to the capturing areas of 2022 and 2023 not having maximum achievable spatial overlap (see Section 4.2). When looking at Figure 10 it seems more likely, that simply more devices of MAN1, who uses proper encryption, were captured in 2023, explaining the difference.

As it can be seen in Figure 10, the use of encryption differs greatly from manufacturer to manufacturer. While we almost exclusively recorded encrypted devices from MAN1, MAN4, and MAN5, the devices of MAN2 and MAN3 mostly do not use encryption.

Within this context, it is important to note that the choice in which encryption mode the devices are operated in is made by the operator (metering provider). The depicted manufacturers here cannot always influence in which modes their devices are used. The responsibility for resolving the problem of missing encryption therefore lies with the metering point operators.

Evolution of encryption from 2022 to 2023. When comparing the results of the two years, the difference is almost negligible. In relation to the other encryption states, the number of not-encrypted and not-interpreted transmitting devices has decreased. At the same time, more devices with Mode 7 were recorded. However, when looking at Figure 10 the general tendency of the implementation of encryption or lack thereof per manufacturer seems to have remained unchanged. Regarding RQ3, it can be concluded that at least the devices of some manufacturers are operated without using encryption.

5.4 Impact on Privacy

Finally, the impact of unencrypted telegrams on privacy needs to be examined (RQ4). As mentioned in Section 5.3 some unencrypted telegrams can be decoded using data types defined in the standard, while others are proprietary encoded by the manufacturer.

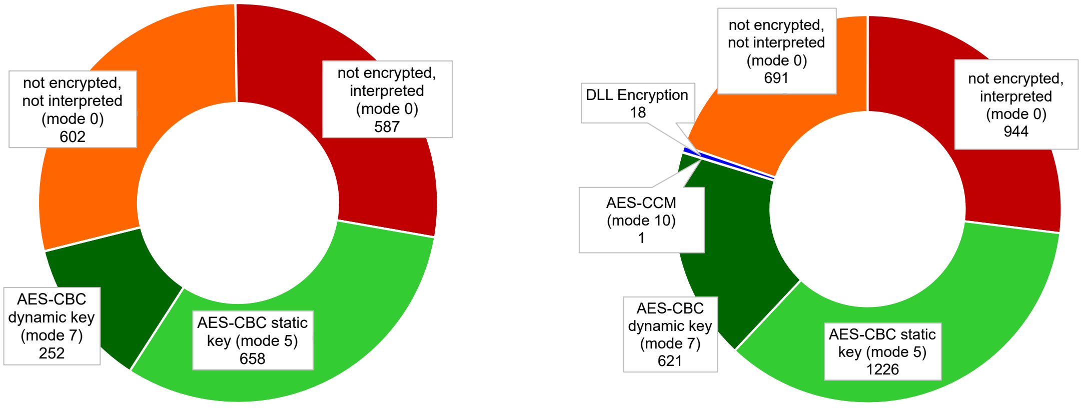
Manufacturer-specific encoding could be a limited protection by security through obscurity. However, we found it to be easy to interpret how a manufacturer-specific data record is structured based on the data physically displayed on the sensor and through visually inspecting the received telegrams. Particularly on newly installed devices, many values are zero in manufacturer-specific data records, which considerably simplifies reverse engineering. To demonstrate the possibility to also decode unencrypted proprietary telegrams, we implemented custom decoders for a limited number of sensor types.

Unencrypted and unsolicited transmission of metering data over the air poses a serious risk to privacy because they open the path to behavioral tracking. Hence, for the present paper, an apartment was sniffed (with the approval of the apartment inhabitants). By the data of one meter, the presence, and the behavior of the inhabitants could be silently tracked without significant effort.

The severity of the sensitivity of the data is highlighted in Figure 11. The heatmap shows the data from one warm water meter that has been tracked for several weeks. Plotted on a heat map, it is easy to identify the periods of high and low consumption. Consequently, it can be concluded that the apartment was probably empty between the 2023-06-05 and the 2023-06-12. Furthermore, it can be stated that the inhabitant usually sleeps between midnight and 7 a.m. to 10 a.m. in the morning.

In this long-time experiment, only the data from one device were analyzed in detail over a long period. We used the actual metering device installed by the metering point operator in the home of one of the authors. However, based on the results so far, it can be assumed that if a larger number of devices (e.g., from an entire building complex or a street) are recorded, complex and precise behavioral profiles of hundreds of people can easily be created.

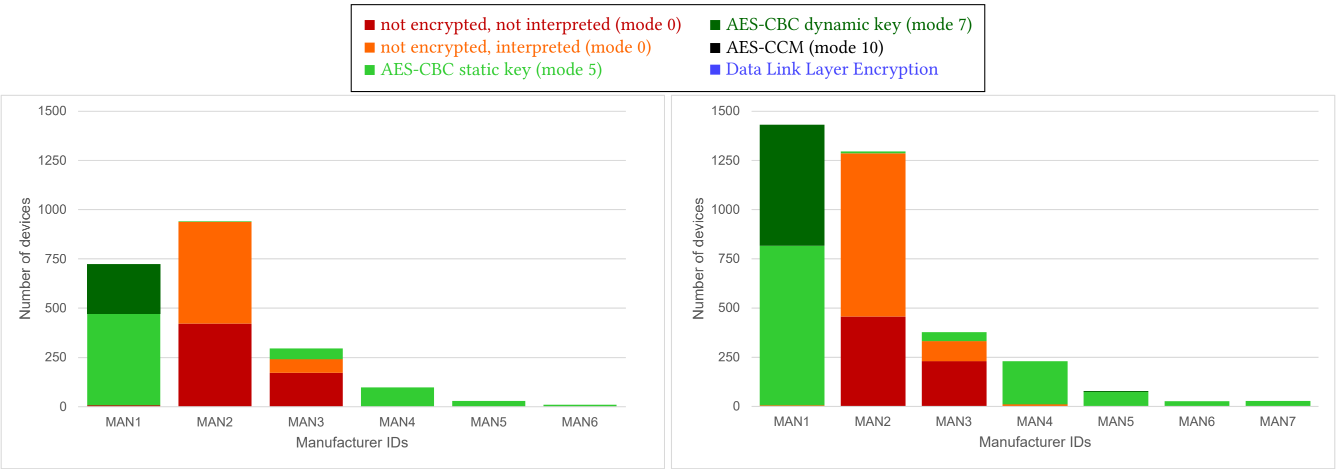
These could then allow statements to be made about the number of people, their presence, and absence, their sleeping and rising times, and their heating and showering behavior. It is even possible to track whether inhabitants stay out at night and use the bathroom. Detailed monitoring of residents is therefore possible.



(a) Encryption mode usage in 2022

(b) Encryption mode usage in 2023

Fig. 9. Number of Devices ordered according to the Encryption Method. About half of all devices are not encrypted, and of those about half were directly interpretable without additional effort of implementing manufacturer-specific data formats. No significant change can be detected between 2022 and 2023.



(a) Encryption modes used by manufacturers in 2022

(b) Encryption modes used by manufacturers in 2023

Fig. 10. Number of sensors with encryption modes grouped by manufacturer. Manufacturers observed less than five times in a given year are not shown.

If one goes further, one can probably also determine social demographic factors such as age, employment status, number of people in the household, etc. with a more in-depth data analysis.

To summarize, we can answer RQ4 (Do the unprotected telegrams or unprotected telegram parts expose sensitive data?) as follows: Based on the results of the field study regarding the encryption status and the results of the sniffing experiment, it must be stated that even one single unencrypted water meter makes extensive personal data publicly accessible. Without effective encryption, anyone with the simplest hardware can spy on people and households anonymously and discreetly. Privacy is therefore by no means guaranteed. For this reason, all meters must transmit in encrypted form, even though this is only one prerequisite for protecting the personal rights of inhabitants.

6 DISCUSSION AND OUTLOOK

This field study is a first investigation on the usage of wM-Bus in the real world, focusing on the privacy aspect. Although we do not claim the study to be either representative or comprehensive due to the following reasons, the results still show that noteworthy shortcomings are threatening the privacy of tenants using wM-Bus metering.

Spacial Scope of the Field Study. The first limitation of this paper lies in the scope of the field study. Data were only collected in three southern German federal states and Luxembourg. Market participants that only operate in other federal states are therefore excluded from this study.

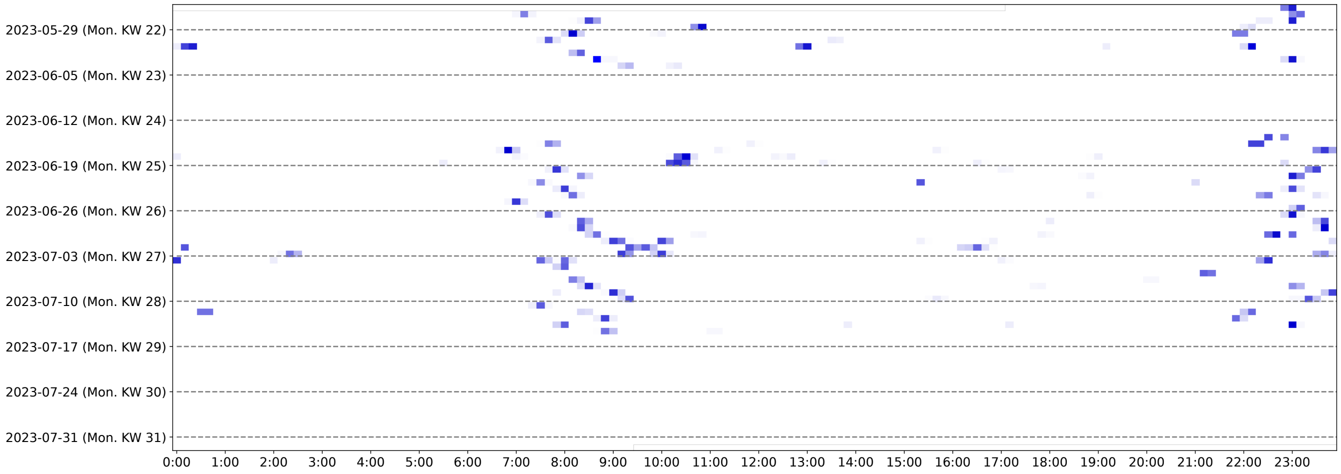


Fig. 11. Heatmap of daily warm water usage. Lines marking the weeks. The absence of the inhabitant in calendar week (KW) 23 as well as the weekly rising and sleeping pattern is clearly visible.

Deviation of Observed Market Share and Expected Market Share. Using our more comprehensive non-pseudonimized data set, we compared the manufacturers' names[5] with the existing market environment. Some well-known manufacturers of wireless metering devices were not present. This suggests that different manufacturers may use different operating modes or operate in different areas not covered by our study.

Distribution of Metering Devices. 4.986 metering devices were identified, most of which were heat cost allocators. The majority of data was recorded in the Munich city center/west area, where a travel distance of around 65 km was covered. In addition, routes were traveled in southern Munich, Karlsruhe, Trier, and Luxembourg. In total, a distance of more than 100 km was covered, which led to the desired spread of the measuring points and thus also to an extrapolation of the data.

Duration of Stay. Frequent transmission may not be often enough that a walk along the street was able to capture all sensors of the buildings. It also has to be mentioned that not the same walking path was traversed in 2022 and 2023. And no systematic methodology was employed to ensure the comprehensive capture of all existing devices (such as duration of stay, consistent route, etc.).

Telegram loss. In a stationary experiment with more than 100 devices, we noticed that some devices were only received for the first time after more than an hour, although it was ensured that these devices were all transmitting at the same rate of 3 Minutes. We assume that these devices were lost due to telegram collisions or other physical limitations in the wireless transmission. This suggests that a certain number of devices were also missed in the field study due to telegram collision or physical limitations.

Restrictions on Operating Modes. Due to the configuration of the hardware, only telegrams with transmission mode C1 or T1 were recorded. C1 and T1 are unidirectional transmission modes (as described in 3.2.1). Devices for which the transmission has to be requested using bidirectional communication are therefore not recorded (mode C2 / T2). Communication modes apart from C and T (e.g., N, S, R and F) were not considered in this study. The limitations mean that the results presented in this work relate exclusively to modes C1 / T1 and conclusions about devices with other transmission modes are inadmissible.

Decryption of encrypted telegrams. Decryption of telegrams was not considered in this work. However, it is theoretically possible that telegrams can be easily decrypted if the operator uses a weak key or a single key for all devices. This would mean that not only the unencrypted half of the devices examined in this study would represent a security risk for privacy, but also the supposedly securely encrypted devices would reveal private data.

Outlook

The implementation of this field study only provides a first investigation of how wM-Bus is used in real-world applications. We propose the following ideas for improvement in future work.

- **Increase sample size** The field study was only conducted in three urban areas in Germany and one in Luxembourg. It is known to the authors that metering operators and deployed sensor devices vary between cities and federal states. For a representative field study, more cities from different states and countries should be considered.
- **Wireless M-Bus Modes** This work focused on the wM-Bus modes C1 and T1. Other modes of operation should be considered in future campaigns to get a comprehensive view of the wM-Bus usage.
- **Software Defined Radio** Software Defined Radio (SDR) facilitates the simultaneous recording of multiple wM-Bus

[5] https://www.dlms.com/flag-id-directory/

modes at once. This alleviates some limitations of the presented study and enables future studies using inexpensive hardware.
- **Secret Key Management** As highlighted by [14], the wM-Bus standard proposes disadvantageous methods for the management of the wM-Bus encryption keys. It would be of interest to investigate weaknesses in how secret keys are handled in the field by the operator and manufacturers.

7 DISCLOSURE PROCESS

In the process of this field study, we informed all wireless M-Bus manufacturers from which we have captured telegrams, and operators known to us prior to the publication of this paper and requested comments. Only one manufacturer replied, commenting their devices strictly uses encryption. We could confirm that in our dataset.

In this study, we did not attempt to break any protection mechanisms like the decryption of the encrypted telegrams, and we collected all telegrams by listening to openly non-directionally broadcasted telegrams only. Only the non-directional, public telegrams from sending mode 44_h were recorded (see also Section 3.2.2). These are telegrams that can be read by anyone.

It is infeasible to coordinate a remedy for the issues demonstrated in this study, as it would require the physical exchange of many sensors. With this publication, we hope to promote the usage of adequate encryption and privacy protection in the future.

8 CONCLUSION

Our field study analyzed an untargeted sample of the real-world usage of wireless M-Bus (wM-Bus) in Germany and Luxembourg in 2022 and 2023 with the goal to expose the existence of security or privacy risks. We created a portable device to capture wM-Bus sensor telegrams which are broadcasted frequently. Using the device, we walked through four urban areas and recorded broadcasted wM-Bus telegrams as well as the position where the telegram was received. Almost 5000 unique sensor devices were identified throughout all campaigns. The application of the sensors was identified by decoding the transmitted device type of each sensor. Demonstrating, we were able to capture, interpret and spatially allocate wM-Bus telegrams (RQ2).

We displayed a statistic of how often encryption was used to protect the metering information. We described the capturing process, the used hardware, and the relevant parts of the wM-Bus standard which we used to derive our statistics. To our surprise, we found that about half of the metering devices do not use encryption (RQ3) to protect the privacy of the apartment inhabitants. We demonstrated that non-encrypted metering data transmitted by a commercially available wM-Bus sensor poses a privacy threat (RQ4). To conclude, we found no inherent flaws in the design of the wM-Bus protocol that poses a practical risk to privacy. However, our sample of wM-Bus usage in practice demonstrated that misconfiguration puts the privacy of inhabitants of apartment buildings at risk (RQ1).

The major contributions of this paper are:

- We showed that about half of the wireless sensors in real-world use do not use encryption (Section 5.3).
- The non-encrypted telegrams can be captured in a short interval (5 - 15 min) and most telegrams can be decoded easily.
- The decoded data enables precise tracking of inhabitant behavior.

We want to raise awareness of existing privacy problems in the real-world usage of wM-Bus and point out that standards exist that protect privacy. Especially BSI-TR-03109-1[6] requires wM-Bus using encryption mode 7 if these devices are to be integrated into the German Smart Metering System. This study highlights the necessity of binding requirements, as manufacturers and operators do not always implement privacy-friendly solution on their own initiative. As discussed in Section 6, further investigation needs to be conducted to create a comprehensive data set of wM-Bus usage to representatively quantify the real dimension of the identified privacy concern.

ACKNOWLEDGMENTS

This work was supported by the project 'Smart East'[6] (funding reference L75 21113 by Ministerium für Umwelt, Klima und Energiewirtschaft Baden-Württemberg) as well as by the Helmholtz Association under the programs 'Energy System Design (ESD)' (topic number 37.12.01) and 'Engineering Digital Futures (EDF)' as part of the KASTEL Security Research Labs, Karlsruhe (topic number 46.23.02).

AUTHOR CONTRIBUTIONS

Author contributions according to Contributor Roles Taxonomy (CRediT, https://credit.niso.org/): *Conceptualization:* F.H.; *Methodology:* F.H.; *Software:* F.H.; *Formal analysis:* F.H.; *Investigation:* F.H.; *Data curation:* F.H.; *Writing - original draft:* F.H., K.B., J.G.; *Writing - review and editing:* F.H., K.B., J.G., S.W., V.H.; *Visualization:* F.H., K.B.; *Supervision:* J.G., S.W., V.H.; *Funding acquisition:* V.H.

REFERENCES

[1] Wafaa Anani and Abdelkader Ouda. 2022. Wireless Meter Bus: Secure Remote Metering within the IoT Smart Grid. en. In *2022 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, Shenzhen, China, (July 2022), 1–6. ISBN: 978-1-66548-544-9. DOI: 10.1109/ISNCC55209.2022.9851807.

[2] Muhammad Rizwan Asghar, Gyorgy Dan, Daniele Miorandi, and Imrich Chlamtac. 2017. Smart Meter Data Privacy: A Survey. *IEEE Communications Surveys & Tutorials*, 19, 4, 2820–2835. DOI: 10.1109/COMST.2017.2720195.

[3] Carsten Bories. 1995. *Einrichtung Einer Intelligenten Ausleseeinheit Für Verbrauchsmeßzähler.* Diploma Thesis. (Mar. 1995).

[4] Cyrill Brunschwiler. 2013. Wireless M-Bus Security Whitepaper Black Hat USA 2013 June 30th, 2013. https://www.compass-security.com/fileadmin/Datein/Research/Praesentationen/blackhat_2013_wmbus_security_whitepaper.pdf.

[5] Feng Chen, Jing Dai, Bingsheng Wang, Sambit Sahu, Milind Naphade, and Chang-Tien Lu. 2011. Activity Analysis Based on Low Sample Rate Smart Meters. In *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. KDD '11: The 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, San Diego California USA, (Aug. 21, 2011), 240–248. ISBN: 978-1-4503-0813-7. DOI: 10.1145/2020408.2020450.

[6] Bundesamt für Sicherheit in der Informationstechnik. 2021. Technische Richtlinie BSI TR-03109-1. Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems. Version 1.1 (6b75fb88). (2021). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109-1.pdf?__blob=publicationFile&v=4.

[6] https://smart-east-ka.de/

[7] HeizkostenV. 2023. Verordnung über Heizkostenabrechnung in der Fassung der Bekanntmachung vom 5. Oktober 2009 (BGBl. I S.3250), die zuletzt durch Artikel 3 des Gesetzes vom 16. Oktober 2023 (BGBl. 2023 I Nr. 280) geändert worden ist. (2023). Retrieved Apr. 18, 2024 from https://www.gesetze-im-internet.de/heizkostenv/HeizkostenV.pdf.

[8] Mikhail A. Lisovich, Deirdre K. Mulligan, and Stephen B. Wicker. 2010. Inferring Personal Information from Demand-Response Systems. *IEEE Security & Privacy*, 8, 1, 11–20. doi: 10.1109/MSP.2010.40.

[9] Pavel Masek, Martin Stusek, Krystof Zeman, Radek Mozny, Aleksandr Ometov, and Jiri Hosek. 2019. A Perspective on Wireless M-Bus for Smart Electricity Grids. In *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*. 2019 42nd International Conference on Telecommunications and Signal Processing (TSP). IEEE, Budapest, Hungary, (July 2019), 730–735. isbn: 978-1-72811-864-2. doi: 10.1109/TSP.2019.8768840.

[10] Pavel Masek, Krystof Zeman, Zenon Kuder, Jiri Hosek, Sergey Andreev, Radek Fujdiak, and Franz Kropfl. 2016. Wireless M-BUS: An Attractive M2M Technology for 5G-Grade Home Automation. In *Internet of Things. IoT Infrastructures*. Vol. 169. Benny Mandler et al., (Eds.) Springer International Publishing, Cham, 144–156. isbn: 978-3-319-47062-7 978-3-319-47063-4. doi: 10.1007/978-3-319-47063-4_13.

[11] MessEV. 2024. Mess- und Eichverordnung vom 11. Dezember 2014 (BGBl. I S. 2010, 2011), die zuletzt durch Artikel 1 der Verordnung vom 29. Januar 2024 (BGBl. 2024 I Nr. 27) geändert worden ist. (2024). Retrieved Apr. 18, 2024 from https://www.gesetze-im-internet.de/messev/MessEV.pdf.

[12] Libor Polčák and Petr Matoušek. 2022. Metering Homes: Do Energy Efficiency and Privacy Need to Be in Conflict?: en. In *Proceedings of the 19th International Conference on Security and Cryptography*. SCITEPRESS - Science and Technology Publications, Lisbon, Portugal, 47–58. isbn: 978-989-758-590-6. doi: 10.5220/0011139000003283.

[13] Huwida Said, Mario Guimaraes, Noora Al Mutawa, and Ibtesam Al Awadhi. 2011. Forensics and War-Driving on Unsecured Wireless Network. In *2011 International Conference for Internet Technology and Secured Transactions*. 2011 International Conference for Internet Technology and Secured Transactions. (Dec. 2011), 19–24.

[14] Peter Shipley. 802.11b War Driving and Lan Jacking. (2001). Retrieved Apr. 3, 2023 from https://www.youtube.com/watch?v=bWH-3OZJ0vo.

[15] S. Spinsante, S. Squartini, L. Gabrielli, M. Pizzichini, E. Gambi, and F. Piazza. 2014. Wireless M-Bus Sensor Networks for Smart Water Grids: Analysis and Results. *International Journal of Distributed Sensor Networks*, 10, 6, (June 1, 2014), 579271. doi: 10.1155/2014/579271.

[16] Susanna Spinsante, Mirco Pizzichini, Matteo Mencarelli, Stefano Squartini, and Ennio Gambi. 2013. Evaluation of the Wireless M-Bus Standard for Future Smart Water Grids. In *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*. 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC 2013). IEEE, Sardinia, Italy, (July 2013), 1382–1387. isbn: 978-1-4673-2480-9 978-1-4673-2479-3 978-1-4673-2478-6. doi: 10.1109/IWCMC.2013.6583758.

[17] S. Squartini, L. Gabrielli, M. Mencarelli, Mirco Pizzichini, S. Spinsante, and F. Piazza. 2013. Wireless M-Bus sensor nodes in smart water grids: The energy issue. *2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP)*, 614–619. doi: 10.1109/ICICIP.2013.6568148.

Received 19 April 2024; revised 2 August 2024; accepted 17 June 2024

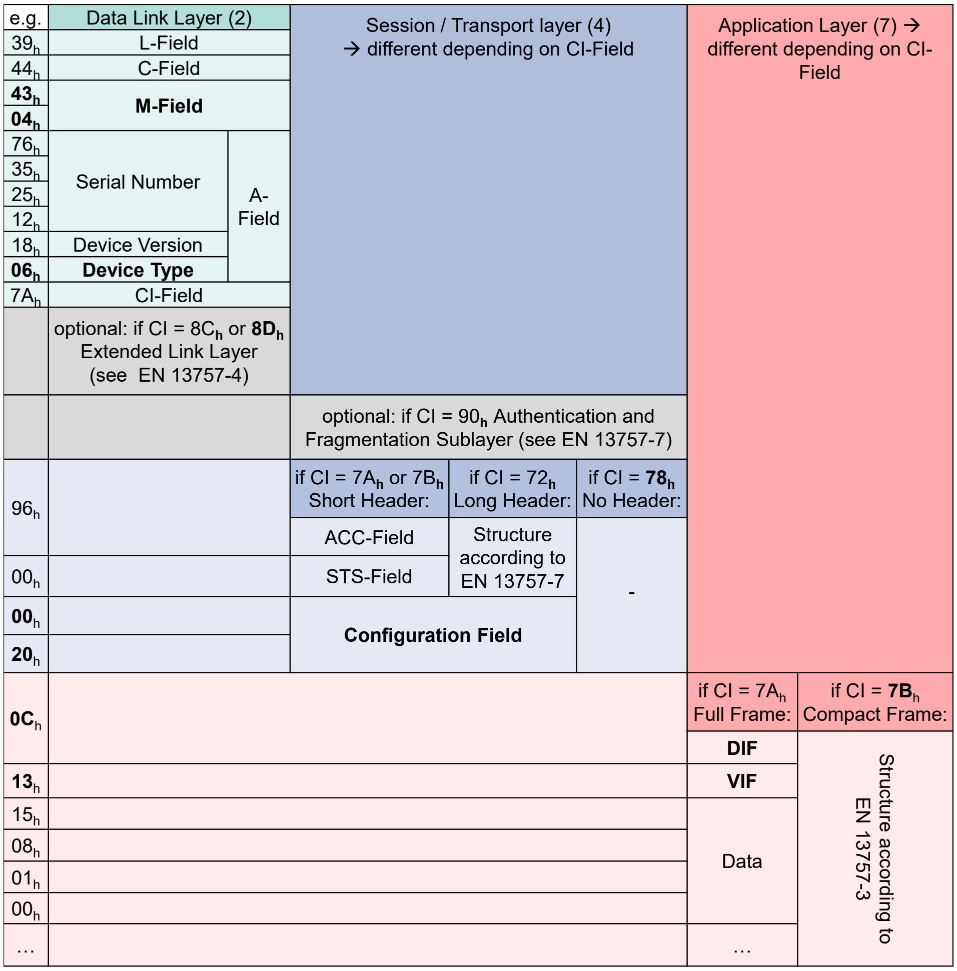


Fig. 12. M-Bus telegrams and variations depending on the value of the CI fields. **Bold** font marks data that is used to derive the results shown in Section 5.