Bit- and Symbol-Error Patterns in IEEE 802.15.4 TSCH Mode

Fabian Graf, Thomas Watteyne, Filip Maksimovic, Michael Villnow

Bit- and Symbol-Error Patterns in IEEE 802.15.4 TSCH Mode

Fabian Graf
Siemens AG
Siemens Technology
Erlangen, Germany
fabian.graf@siemens.com

Thomas Watteyne
Inria
AIO Team
Paris, France
thomas.watteyne@inria.fr

Filip Maksimovic
Inria
AIO Team
Paris, France
filip.maksimovic@inria.fr

Michael Villnow
Siemens AG
Siemens Technology
Erlangen, Germany
michael.villnow@siemens.com

***Abstract*—Bit errors in wireless communication predominantly stem from external interference as well as from multipath fading and attenuation. In order to tackle these harmful influences, the IEEE 802.15.4 standard includes time slotted channel hopping. We have collected packets containing bit errors from 200,000 packets generated in two different testbeds. We show that the channels used in IEEE 802.15.4 exhibit different error patterns typical for either external interference or multi-path fading and attenuation. These insights allow to detect, classify and quantify the presence of these phenomena. Furthermore, practical use cases for exploiting the knowledge on error patterns on a per-channel basis are presented. We propose to choose Forward Error Correction on a per channel basis and provide reference values in terms of code error correcting capability required to recover from 50% of the occurred packet errors on certain channels.**

I. Introduction

IEEE 802.15.4 [1] has turned into the de-facto standard for low-power wireless networks. Besides the low-power characteristic, reliability is the most important feature in these kind of Industrial Internet of Things (IIoT) networks, according to the customers [2]. A strategy called time slotted channel hopping (TSCH) has proven to deliver a significant performance boost in terms of reliability [3]. The idea of TSCH is to cut time into time slots and the available frequency band into channels. The nodes in the network consequently transmit and receive based on a communication schedule at a certain time and frequency. By iteratively changing channels, frequency diversity can be exploited to combat the two most common reasons causing a wireless transmission to fail: external interference and multipath fading and attenuation (MFA). Thus, TSCH has been included at first as an amendment into IEEE 802.15.4e [4] and later in its entirety into IEEE 802.15.4-2015 [5].

Besides being a dependable technology, Application Performance Monitoring (APM) has turned out to be another key factor of achieving reliability. The goal of APM is to provide a current status on the health condition of the system to the user. Especially in low-power wireless systems, the verbosity of these status reports is usually sparse due to several resource constraints related to cost and size. Power consumption, bandwidth allocations and device storage often limit the networking metrics reported to the user to reliability and packet delivery ratio (PDR), at best. While reliability determines how many packets actually get lost, e.g. due to exceeded retry count, the PDR also accounts for the failed attempts to deliver the packet. However, the user still has no hint on the error source, i.e. whether the packet was lost due to poor signal strength or a failed Cyclic Redundancy Check (CRC). According to IEEE 802.15.4 packets with a failed CRC are immediately discarded. In reality, the knowledge on symbol error positions is extremely valuable. The gained insights would enhance strategies for error correction and give hints on the presence of external interference and MFA. Obviously, these insights can only be gathered by means of a genie-aided approach knowing the originally sent packets. Nonetheless, in practical scenarios, the understanding of error patterns can be approximated by strategies based on a predefined set of sequences known to transmitter and receiver, respectively.

In this paper, we present such bit- and symbol-error patterns collected from erroneous transmissions in two different real-world IEEE 802.15.4 testbed deployments. The novelty of our work is the collection and analysis of error patterns across all 16 channels offered by IEEE 802.15.4. While several studies on the PDR of these channels exist, we deliver a comprehensive study on the absolute number and shape of bit- and symbol-errors across the channels for the first time. Based on this study, we are capable of detecting, classifying and quantifying the presence of external interference and MFA in our test setups. Primarily, we show how, based on error patterns, their harmful influence on the transmission varies when TSCH is applied. On top of that, this article features practical approaches on exploiting this knowledge in real-world scenarios by paving the path for a channel-dependent Forward Error Correction (FEC) algorithm.

The remainder of this paper is organized as follows. Section II provides an overview of the technical specifications of IEEE 802.15.4 and related work on analysis of transmission errors. Section III presents the used hardware (HW) setup and the used testbed deployments. Section IV analyses collected error patterns and the receive signal strength indicator (RSSI) across the different IEEE 802.15.4 channels. Section V discusses the practical use of the gained insights. Section VI concludes the paper and presents outlook on future work.

II. Transmission Errors in IEEE 802.15.4

The technical specification of the IEEE 802.15.4 standard already includes methods for transmission error detection and correction, respectively. Thus, we briefly present the communication chain of a packet in Section II-A. Naturally, the wireless medium may cause transmissions to fail. Section II-B presents related work on induced error patterns.

A. Communication Chain in IEEE 802.15.4

Packets in IEEE 802.15.4 follow a fixed structure, which already defines the size and arrangement of the header and payload fields on the MAC layer. Based on the MAC header and MAC payload, a 2 B long CRC is computed and appended, as a Frame Check Sequence (FCS) field behind the payload. The arising structure, the MAC protocol data unit (MPDU), is at most 127 B long and handed as PHY service data unit (PSDU) to the PHY layer. In a next step, the frame length field (1 B) is added just before the PSDU. Finally, a preamble sequence (4 B) and a start of frame delimiter (SFD) (1 B) are put in front as synchronization header fields. The resulting complete frame, the PHY protocol data unit (PPDU), ends up to be at most 133 B long and is converted into hexadecimal symbols before being passed to the Direct Sequence Spread Spectrum (DSSS) mapper. DSSS maps each 4 bit hexadecimal symbol into one of 16 nearly-orthogonal pseudo-noise (PN) code sequence, each 32 chips long. The resulting 32 chips per symbol are then modulated on a half sine pulse using Offset-Quadrature Phase Shift Keying (O-QPSK). The carrier frequency f_c of the waveform is defined by the selected IEEE 802.15.4 channel number in the range between 11 and 26, i.e.

$$f_c = 2405 + 5(k - 11) \text{ MHz, for } k \in \{11, \ldots, 26\}. \quad (1)$$

After demodulation, the received chip sequence is passed to the DSSS de-mapper. A maximum likelihood (ML) decoder deciding on the minimum hamming distance between the received chip sequence and the 16 PN-code sequences is used. With a rising number of Chip Errors per PN-Code (CEPP), the probability that the ML decoder in DSSS decides for a wrong PN sequence grows [6]. Thus, after removing the PHY Header fields, a CRC check is performed to detect these errors. If the CRC check fails, the packet is discarded and the packet is re-transmitted following the automatic repeat request (ARQ) principle. The transmission chain is depicted in Fig 1.

B. Related Work

Considering the long time since the IEEE 802.15.4 standard has been launched, there is surprisingly little literature on the characteristics of transmission errors.

Pešović et al. [7] derive an analytical expression on the chip error probability (CEP) in IEEE 802.15.4 based on theoretical simulations over an Additive White Gaussian Noise (AWGN) channel. Later, the authors extended the results by deriving the probability for a symbol error in terms of the CEPP.

Wu et al. [8] provide a detailed study on chip error patterns in IEEE 802.15.4. By analysing the distribution of the CEPP positions across the packet, the authors identify four major error patterns. The distribution of these error patterns varies with changing environments, for which either external interference or MFA are the dominant sources of error. Furthermore, knowledge on chip error patterns can be used for reactive jamming detection [9].

However, such investigations on chip errors can only be conducted by means of software defined radios, since DSSS and also CRC is done in HW due to performance reasons.

Barac et al. [10] deliver comprehensive bit- and symbol-level analysis of IEEE 802.15.4 transmission errors in industrial environments. Typical bit-error patterns for external interference and MFA based on a large amount of packets sent in real-world industrial testbeds are shown. Besides that, the authors highlight properties of error-bursts, i.e. the bit errors often appear to occur in blocks instead of being spread across the packet. On top of that, the findings are used to develop FEC coding schemes combined with interleaving. The same authors also use these information on error patterns and introduced the Lightweight Packet Error Discriminator (LPED), that distinguishes between errors caused by MFA and external interference [11], [12]. Although these studies cover transmissions across all available channels in IEEE 802.15.4, there is no analysis on how the patterns evolve in a TSCH scenario on a per-channel basis.

Brun-Laguna et al. [13] offer a detailed analysis on PDRs over the different IEEE 802.15.4 channels based on statistics gathered from 6 different testbeds. Their results directly show the harmful effects of interference on the channels, which are also occupied by IEEE 802.11. However, the results lack of an analysis on a symbol- and bit-level, respectively.

Ilyas and Radha [14] investigate the Bit Error Rate (BER) for IEEE 802.15.4 channel 26 as it is the channel in the frequency spectrum that is the farthest removed from all IEEE 802.11 frequency channels. Although the authors later extend their studies to all 16 available IEEE 802.15.4 channels, their analysis is rather limited to BER than on actual error patterns [15].

III. Experimental Setup

In order to collect a large set of error patterns, we set up two experimental testbeds based on microcontroller units (MCUs) with IEEE 802.15.4 compliant radios. In Section III-A the chosen MCU architecture, the used firmware (FW) and the test automation framework is introduced. Section III-B shows the environments selected for data collection.

A. Hardware Setup

In our experiments, we use nRF52840-DK boards from Nordic Semiconductor. The MCU relies on a 64 MHz Arm Cortex-M4 architecture and has access to a IEEE 802.15.4 compliant 2.4 GHz radio. The radio transmit power is adjustable between -20 dBm and +8 dBm. For our investigations, we drive the radio at 0 dBm exclusively. The development kit (DK) version of nRF52840 additionally offers an on-board J-Link debugger for programming via USB. This USB

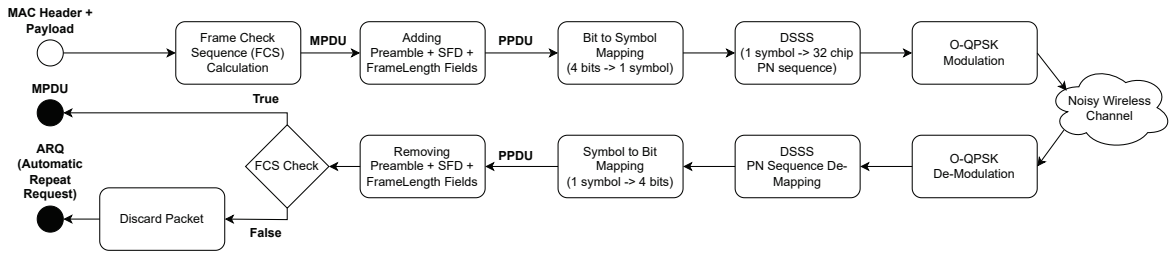

Figure 1: Communication chain of a packet through the wireless channel according to IEEE 802.15.4.

port is also used to control the FW running on the chips, which triggers the radio during test. Our FW sets up on a Nordic sample application, called *IEEE 802.15.4 PHY Test Tool (PTT)* [16]. The PTT runs as an application based on *Zephyr* and is controlled via a command line interface (CLI). A large set of functions to experiment with the IEEE 802.15.4 radio is provided as part of the PTT, such as setting transmit power or switching to receive mode or transmit mode. In our use-case, we set one device into transmit mode, i.e random payloads of custom size (125 B) are continuously generated and transmitted with an adjustable time period. The other devices act in receiver mode: they switch on their radio all the time with a receiver sensitivity of -100 dBm and sniff all incoming packets. To analyze bit error patterns, the transmitter and receiver send their transmitted and received packets via the CLI, too. A Python test automation script stores the payload to log files and adds some meta-information from the receiver PTT. This meta-data includes the used channel, the RSSI and the result of the CRC check. By default, packets with failed CRC would be immediately discarded according to the standard. Therefore, we adjust the radio driver to ignore the failed CRC. This function is called in the interrupt handler for a failed CRC check and fetches the erroneous packet from the packet pointer register.

The PTT offers the possibility to switch between the 16 different IEEE 802.15.4 channels. In order to ensure a transmit and receive operation on the same channel, the Python test automation scripts agree via SSH on a common channel. We decide to send one packet every 500 ms and to switch the channel after every 20 transmitted packets to get a trade-off between generating a sufficiently large set of data and mimic a TSCH-like behavior as good as possible.

Finally, at the end of the test, the log files of the transmitter and receiver are passed to a Python based packet analyzer script, which compares transmitted and received payloads to identify correct and erroneous packets. It also identifies interfering packets, which are accidentally sniffed by the receiver. The full test setup is shown in Fig. 2.

B. Testbeds

The described HW setup is deployed in two different testbeds. In the apartment test environment, the transmitter and receiver are placed in different rooms with no line-of-sight (LOS) in a distance of about 10 m. A single Wi-Fi router

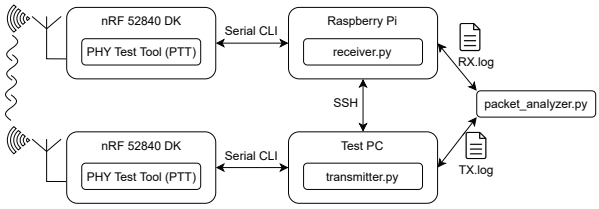

Figure 2: Test Setup consisting of nRF boards running a PHY Test Tool based on Zephyr.

and some Smart-Home gadgets may be sources of external interference in this testbed. Several walls and doors between transmitter and receiver are likely to result in MFA.

For the industrial lab environment, a sensor application lab has been chosen. Again the devices are placed in similar distance as in the apartment setup, however, with almost LOS. The lab is a large experimentation area with a couple of desks separated by some wooden partition walls. Tons of different smart field devices as well as office Wi-Fi routers run in this lab resulting in a high amount of external interference.

IV. Bit- and Symbol-Error Pattern Analysis

In both testbeds, 100.000 packets, each with a PPDU payload size of 125 B, have been transmitted in experiments covering several days. The resulting error packets are analyzed in terms of conspicuous patterns in Section IV. Section IV-B shows the evolution of the RSSI over time. Besides the typical characteristics of channel hopping, the RSSI statistics also reveal interesting facts about some interfering sources in terms of distance and activity, which can be inferred from the sniffed packets by the receiver.

A. Error Pattern Types

When studying the error positions of erroneous packets, i.e. comparing packets with a failed CRC with the originally transmitted sequence symbol by symbol, two types of error patterns can be surprisingly clearly distinguished. The results unambiguously confirm the findings by Barac et al. [10].

The first kind of patterns consists of a relatively small number of symbol errors, which sometimes appear to occur in small *bursts*. Occasionally, it is just a single error burst as in Fig. 3 (a) that causes the CRC to fail and the whole packet to be corrupted. However, more often, single symbol errors or several small error bursts can be discovered which are

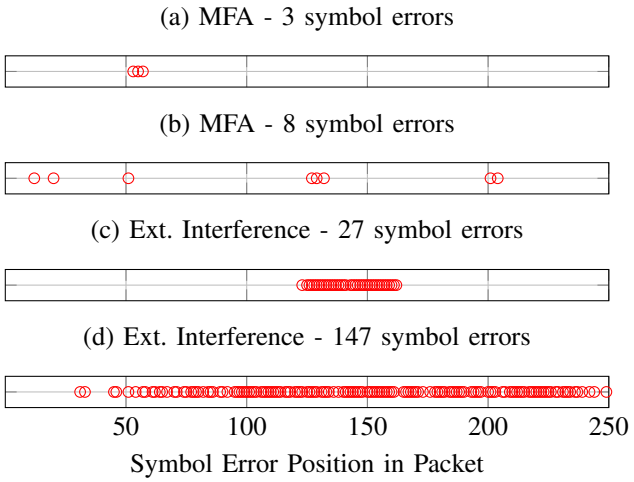

Figure 3: Typical Error Patterns in IEEE 802.15.4.

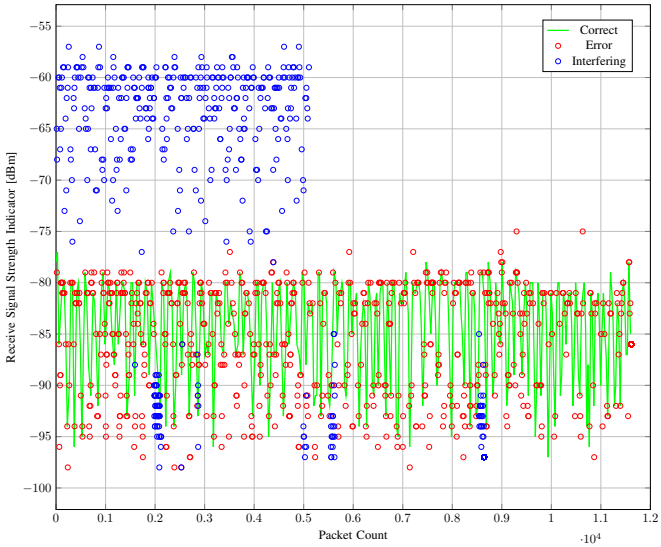

Figure 4: Receive Signal Strength Indicator (RSSI) over time

randomly placed as in Fig. 3 (b). These kind of error patterns most likely stem from MFA distortions.

The second sort of patterns is characterized by a much larger number of symbol errors. The errors do not occur in small bursts, but seem to start at a certain symbol position and then pull through for a large number of consecutive symbols as in Fig. 3 (c) or often even to the end as shown in Fig. 3 (d). Regardless how early the first symbol error occurs, the receive process does not seem to recover from this type of error source. These densely packed patterns are typical signs of external interference.

When converting the error patterns in the binary domain, each symbol error may stretch across 4 consecutive bit positions, since 4 bits are encoded into one PN-sequence.

B. RSSI Analysis in Channel Hopping Mode

As a next step, we analyze the occurrence of these corrupted packets over time, in order to get a better understanding of the environment. It turns out to be helpful to plot also the RSSI of all the received packets over time, as in Fig. 4, belonging to the lab testbed. The green plot shows the RSSI of all correct transmissions. A narrow zig-zag structure immediately becomes visible. This hopping between RSSI levels is directly related to the channel hopping mechanism implemented in the test automation script, which triggers the PTT running on the nRF52840-DK to switch channels incrementally, i.e. from 11 to 26, as in TSCH.

In 2012, TSCH has been added to the standard as an amendment as IEEE 802.15.4e [5]. TSCH typically requires all members of the network to be synchronized within μs. This allows to slice up time into time-slots, which are typically 10 ms long [17], and distribute a common schedule across all nodes. By changing the channel according to this schedule, frequency diversity can be exploited to combat external interference [3] and mitigate MFA [18]. The amplitude in terms of RSSI of the captured correctly received packets is approximately 15 dB in this test run. This large RSSI discrepancy between the different channels is not unusual. Values up to even 20 dB are reported in literature [18], [12].

The red dots in Fig. 4 indicate erroneous packets with a failed CRC. The distribution of these packets over time is quite uniform. Furthermore, failed transmissions appear to occur at any RSSI level.

In Fig. 4, there are also groups of blue dots, which belong to received packets, which have not been transmitted by our test setup, i.e. they stem from another interfering source. All these packets have been sniffed by chance and the majority also has passed the CRC check. This is an indicator, that these interfering packets have also been emitted by an IEEE 802.15.4 radio because the same CRC algorithm for the creation of the FCS has apparently been used. The largest group of blue dots is centered around an RSSI of value -60 dBm and is visible just during the first 5,000 received packets. Due to the channel hopping logic of our receiver, the RSSI values also tend to jump between different levels. Apparently, the interfering device has been shut down during our experiment. Nevertheless, no reduction in terms of erroneous packets can be observed afterwards, which leads to the conclusion that this particular application does not seem to have harmful influence on our testbed. However, the interfering source is obviously closer to our deployed receiver compared to the transmitter device based on the absolute RSSI values and assuming that the interferer operates with the same transmit power. Another interfering device can be spotted 3 times during the experiment phase at a packet count of around 2,000, 5,600 and 8,700. The duration at which this device emits packets is rather short and also has no recognizable influence on our experimental results.

C. Error Patterns across the IEEE 802.15.4 channels

In the following, we shift our focus on the erroneous packets. Moreover, we analyze bit- and symbol-error patterns on a per-channel basis. 100,000 packets in total have been transmitted in each testbed, i.e. 6,250 per channel. As expected, the PDR varies across the channels, but in the

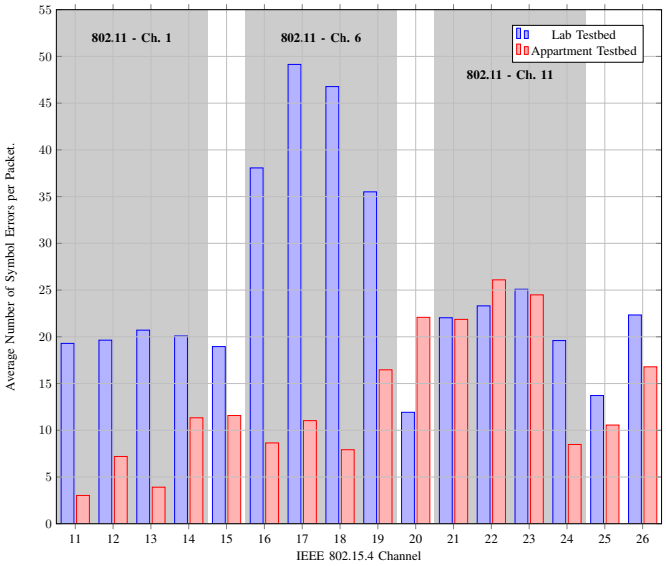

Figure 5: Average number of symbol errors per packet of 125 B ($\widehat{=}$ 250 hex. symbols) across IEEE 802.15.4 channels.

following we report novel findings on the distribution of error patterns, which also varies across the frequency band.

In Fig. 5, we plot the average number of symbol errors per erroneous packet for each channel. Except for channel 22, this average is always higher for the lab testbed compared to apartment testbed. This is intuitive, since the lab environment is much more susceptible to external interference. As stated in Section IV-A, error patterns related to external interference consist of a significantly higher amount of symbol errors in contrast to those patterns related to MFA.

When tracking the distribution of the average number of symbol errors per packet for the lab testbed, several conclusions can be drawn. At first, a remarkable increase in terms of symbol errors is visible for channels 16 to 19. The corresponding frequencies are also covered by channel 6 of the IEEE 802.11 Wi-Fi standard. In this frequency range, the harmful Wi-Fi coexistence has led to many corrupted packets showing the typical interference pattern characteristics. Furthermore, channel 20 has the lowest average number of symbol errors per packet. The investigated error patterns of channel 20 almost entirely consist of some few sparsely distributed error burst across the packets representative for MFA. Lastly, we see a significant increase in average symbol errors per packet for IEEE 802.15.4 channels 21 to 24 again, which share the same frequencies as used in IEEE 802.11 channel 11. The corresponding error patterns are also dominated by external interference properties.

However, the observed trends of the lab testbed do not directly match the ones found in the apartment testbed. Although the majority of error patterns occurred in the apartment testbed are anyway rather subject to MFA than to external interference, the amount of symbol errors per packet for IEEE 802.15.4 channels 21 to 24 is on the same level as for the lab testbed. In fact, IEEE 802.11 channel 11 seems to be the Wi-Fi channel in the apartment testbed, which causes most of the interfering error patterns.

From this section, we can already infer that error patterns vary on a per-channel basis, and that the influence of IEEE 802.11 is individual for each deployment. This is also reported by previous studies on PDRs [13], [3], [15].

V. Practical Use of Knowledge on Channel Error Patterns

The practical value of the awareness of bit- and symbol-error patterns for each channel is obvious: detecting, classifying and quantifying external interference as well as MFA is highly important. Naturally, there is no knowledge of bit- and symbol-error patterns in real-world deployments, since the receiver can not make out the error positions in a corrupted frame. Two approaches to approximate the knowledge on bit error position though are pre-defined pilot sequences and FEC. The idea of pre-defined pilot sequences is to share a set of fixed sequences to all motes. At certain time intervals, these sequences are exchanged with the network neighbors and error positions are spotted and reported. The other idea of using FEC involves encoding and decoding of messages in the network with the same channel code. While the CRC check in IEEE 802.15.4 is just able to detect errors, FEC codes are more powerful and even spot the error positions and correct them, as long as the number of transmission errors has not exceeded the error-correcting capability of the code. This concept is also included in the LPED introduced by Barac et al. [11].

The strategy of FEC is to add redundancy to the message, which helps to recover from errors at the cost of a worse communication rate. Although FEC is not part of the 2.4 GHz O-QPSK PHY in IEEE 802.15.4 by default, there have been efforts concerning MAC-Layer based FEC approaches before [19], [20], [10]. Yu et al. [21] also present an adaptive FEC scheme for IEEE 802.15.4 based on the changing PDR over time. The findings in this paper motivate the use of an adaptive FEC scheme on a per-channel basis, i.e. to employ FEC codes of different error correcting capability depending on the average number of symbol errors in a packet on a channel. In Fig. 6 we refer to the lab testbed and show the percentage of erroneous packets with less than t symbol errors for each channel. Assuming a single FEC code with error correcting capability t is used to encode the MPDU, the percentages in Fig. 6 directly translate into the metric packet salvation ratio (PSR) [10], defined as

$$\text{PSR} = \frac{N_{\text{recovered}}}{N_{\text{corrupted}}}, \tag{2}$$

where $N_{\text{corrupted}}$ is the number of received packets with a failed CRC check due to symbol errors and $N_{\text{recovered}}$ is the number of packets that the FEC code can guarantee to correct. For the IEEE 802.15.4 channels affected by external interference from IEEE 802.11 Ch. 1 and Ch. 11, we observe that an FEC code with error correcting capability $t = 15$ symbols is required to recover from errors introduced in 50% of the erroneous packets. However, for the MFA dominated

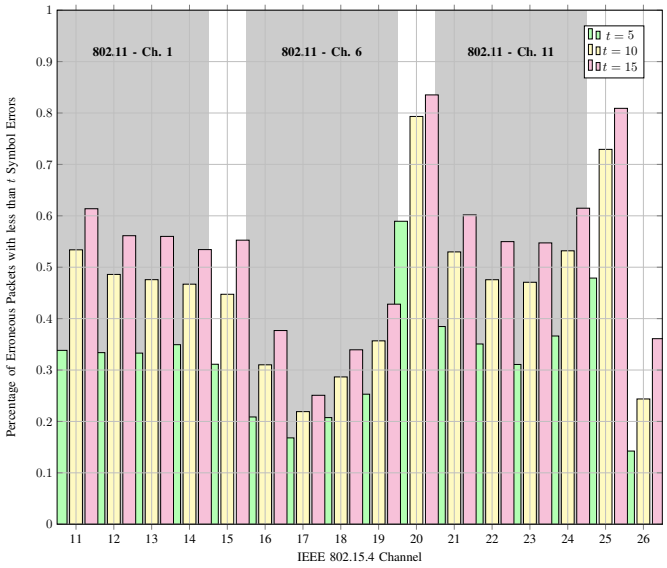

Figure 6: Percentage of erroneous packets in the lab testbed with less than t symbol errors.

IEEE 802.15.4 channels 20 and 25, an FEC code with error correcting capability $t = 5$ is already enough to achieve almost the same PSR.

VI. Conclusion

This study presents bit- and symbol-error patterns observed on the 16 channels used in IEEE 802.15.4-TSCH mode. Based on collecting erroneous packets out of 200,000 packets in two different testbeds, we show that certain channels are affected by different harmful influences, such as external interference and MFA. Consequently, the average number of bit errors and the occurrence of typical error patterns varies in channel hopping scenarios. We also present practical use cases exploiting the knowledge on error patterns. Therefore, we teaser the viability of an adaptive FEC scheme on a per-channel basis to recover from these errors. The design and implementation of such an FEC scheme will be part of future work, as we show that especially for MFA-affected channels, FEC codes with a rather low error correcting capability are sufficient to correct 50% out of all erroneous packets for certain channels. Therefore, more error patterns from further testbeds will be collected as a basis for the scheme's evaluation.

Acknowledgment

This project has received funding from the European Union's Horizon Europe Framework Programme under Grant Agreement No. 101093046.

References

[1] I. C. Society, "IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)," *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, pp. 1–320, 2006.

[2] M. Hatler, "Wireless Sensor Networks: Expanding Opportunities for Industrial IoT," *InTech - ISA's Flagship Publications*, October 2017. [Online]. Available: https://www.isa.org/intech-home/2017/september-october/features/expanding-opportunities-for-industrial-iot

[3] T. Watteyne, A. Mehta, and K. Pister, "Reliability through Frequency Diversity: Why Channel Hopping Makes Sense," in *ACM Symposium on Performance Evaluation of Wireless Ad-hoc, Sensor, and Ubiquitous Networks (PE-WASUN)*, 2009, pp. 116–123.

[4] I. C. Society, "IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements- Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY)- Amendment 1: MAC Sublayer," *IEEE Std 802.15.4e-2012 (Amendment to IEEE Standard 802.15.4-2011)*, pp. 1–225, 2012.

[5] ——, "IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)," *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, pp. 1–709, 2016.

[6] U. Pešović and P. Planinšič, "Error Probability Model for IEEE 802.15.4 Wireless Communications in the Presence of Co-channel Interference," *Physical Communication*, vol. 25, pp. 43–53, 2017.

[7] U. Pešovic, P. Planinšic, and D. Gleich, "Chip Error Probability of IEEE 802.15.4 Wireless Tranmission," in *International Electrotechnical and Computer Science Conference (ERK)*, 2014, pp. 65–68.

[8] K. Wu, H. Tan, H. Ngan, Y. Liu, and L. M. Ni, "Chip Error Pattern Analysis in IEEE 802.15.4," *IEEE Transactions on Mobile Computing*, vol. 11, no. 4, pp. 543–552, 2011.

[9] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. B. Schmitt, "Detection of Reactive Jamming in DSSS-based Wireless Communications," *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1593–1603, 2014.

[10] F. Barac, M. Gidlund, and T. Zhang, "Scrutinizing bit-and symbol-errors of IEEE 802.15.4 Communication in Industrial Environments," *IEEE Transactions on Instrumentation and Measurement*, vol. 63, no. 7, 2014.

[11] ——, "LPED: Channel Diagnostics in WSN through Channel Coding and Symbol Error Statistics," in *IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*. IEEE, 2014, pp. 1–6.

[12] F. Barac, S. Caiola, M. Gidlund, E. Sisinni, and T. Zhang, "Channel diagnostics for wireless sensor networks in harsh industrial environments," *IEEE Sensors Journal*, vol. 14, no. 11, pp. 3983–3995, 2014.

[13] K. Brun-Laguna, P. Gomes, P. Minet, and T. Watteyne, "Moving Beyond Testbeds? Lessons (We) Learned About Connectivity," *IEEE Pervasive Computing*, vol. 17, no. 4, pp. 15–27, 12 2018.

[14] M. U. Ilyas and H. Radha, "Measurement based analysis and modeling of the error process in IEEE 802.15.4 LR-WPANs," in *Conference on Computer Communications (INFOCOM)*. IEEE, 2008.

[15] ——, "Long range dependence of IEEE 802.15.4 wireless channels," in *IEEE International Conference on Communications*, 2008.

[16] Nordic Semiconductors. (2024) IEEE 802.15.4 PHY Test Tool. [Online]. Available: https://developer.nordicsemi.com/nRF_Connect_SDK/doc/latest/nrf/samples/peripheral/802154_phy_test/README.html

[17] D. De Guglielmo, S. Brienza, and G. Anastasi, "IEEE 802.15.4e: A Survey," *Computer Communications*, vol. 88, pp. 1–24, 2016.

[18] T. Watteyne, S. Lanzisera, A. Mehta, and K. S. Pister, "Mitigating Multipath Fading through Channel Hopping in Wireless Sensor Networks," in *IEEE International Conference on Communications (ICC)*, 2010.

[19] K. Yu, M. Gidlund, J. Åkerberg, and M. Bjorkman, "Reliable and Low Latency Transmission in Industrial Wireless Sensor Networks," *Procedia Computer Science*, vol. 5, pp. 866–873, 2011.

[20] K. Yu, F. Baracć, M. Gidlund, J. Åkerberg, and M. Björkman, "A Flexible Error Correction Scheme for IEEE 802.15.4-based Industrial Wireless Sensor Networks," in *IEEE International Symposium on Industrial Electronics*. IEEE, 2012, pp. 1172–1177.

[21] K. Yu, F. Barac, M. Gidlund, and J. Åkerberg, "Adaptive Forward Error Correction for Best Effort Wireless Sensor Networks," in *IEEE International Conference on Communications (ICC)*. IEEE, 2012.