An Analytical Model of Packet Collisions in IEEE 802.15.4 Wireless Networks

Matthias Wilhelm, Vincent Lenders*, and Jens B. Schmitt
Department of Computer Science, TU Kaiserslautern,
67663 Kaiserslautern, Germany
*armasuisse Science and Technology, 3602 Thun, Switzerland

Abstract

Numerous studies showed that concurrent transmissions can boost wireless network performance despite collisions. While these works provide empirical evidence that concurrent transmissions may be received reliably, existing signal capture models only partially explain the root causes of this phenomenon. We present a comprehensive mathematical model that reveals the reasons and provides insights on the key parameters affecting the performance of MSK-modulated transmissions. A major contribution is a closed-form derivation of the receiver bit decision variable for arbitrary numbers of colliding signals and constellations of power ratios, timing offsets, and carrier phase offsets. We systematically explore the root causes for successful packet delivery under concurrent transmissions across the whole parameter space of the model. We confirm the capture threshold behavior observed in previous studies but also reveal new insights relevant for the design of optimal protocols: We identify capture zones depending not only on the signal power ratio but also on time and phase offsets.

I. Introduction

Conventional wireless communication systems consider packet collisions as an evil trait and try to avoid those obstinately by using techniques like carrier sense, channel reservations (virtual carrier sense, RTS/CTS handshakes), or arbitrated medium access (TDMA, polling). The intuition is that concurrent transmissions cause irreparable bit errors at the receiver and render packet transmissions undecodable. However, researchers have found that this model is too conservative. If the signal of interest exceeds the sum of interference of the colliding packets by a certain threshold, packets can in general still be received successfully despite collisions at the receiver. This effect, referred to as the *capture effect* [15], has been explored extensively and validated in many independent practical studies on various communication systems like IEEE 802.11 [7], [9], [13], [14] and IEEE 802.15.4 [8], [17], [25].

Over the past years, the view on packet collisions has therefore changed considerably. Since it is possible for some or even all packets in a collision to survive, there are opportunities to increase the overall channel utilization and significantly improve the network throughput by designing protocols that carefully select terminals for transmitting at the same time [24], [26]. The benefits and potential performance improvements of concurrent transmission are not just of theoretical interest but have been demonstrated practically and adopted in multiple application areas such as any-cast [5] or rapid flooding [6], [16], [27].

Although protocols that exploit concurrent transmissions have shown the potential to boost the overall performance of existing wireless communication systems, their success cannot be explained alone with capture threshold models that are based on the Signal to Interference and Noise Ratio (SINR) [3], [11], [13], [31]. Recent studies have shown that the relative signal powers of colliding packets play an important role in the reception probability but other factors play at least an equally important role in the reception performance. For example, experimental studies in [14], [23] report that the relative timing between colliding packets has a significant influence on the reception probability. Others have reported that the coding [4] or packet content [5] may also greatly influence the reception performance in the presence of collisions. Other factors like the carrier phase offset between a packet of interest and colliding packets also need to be considered as suggested in [20].

In this paper, we strive to provide a comprehensive model accounting for all these factors. Such a model will allow protocol designers to better understand the fundamental root causes and exact conditions under which concurrent transmissions actually work, and thus design optimal protocols based on these factors. While previous studies [9], [17], [28] have also looked at factors that may lead to successful concurrent transmission, these works were either based on practical experiments and have therefore led to empirical models based on measurements which cannot easily be generalized, or derived simplified models that did not account for all the relevant factors (see also Section II). This work advances the field by providing a unified analytical model accounting for all relevant factors and which is not dependent on measurements. Our model ($\rightarrow$ Section III) is based on a mathematical representation on the physical layer using continuous-time expressions of the IQ signals entering the radio interface of a receiver. This fundamental and comprehensive model allows to represent an arbitrary number of colliding packets as a linear superposition of the incoming signals.

A major contribution of this work is a closed-form analytical representation of the bit decision variable at an optimal receiver's demodulator output based on these IQ signals ($\rightarrow$ Section IV). This result enables the deterministic computation of the bit demodulation decision and hence to compute the actual performance of concurrent transmissions for any colliding parameter constellations. Having a bit-level model of reception is not only beneficial for the comprehension of the collision process, it also contributes to areas where a precise bit-level analysis is needed, such as partial packet reception [12] or signal manipulation attacks at the physical layer [20].

Using our model, we explore the parameter space for the reception of MSK-modulated colliding packets for both uncoded systems and DSSS-based systems ($\rightarrow$ Section V), analyzing the parameters' influence on the resulting packet reception ratio (PRR) for concurrent transmissions. While the analysis shows that our model complies with experimental results in the literature, it also provides much more detailed insights into the performance characteristics of novel protocols that exploit collisions. In particular, based on our analysis we identified parameter constellations where concurrent transmissions work particularly reliably. We therefore propose a generalization of the traditional capture threshold model based on the signal power towards a *capture zone*. Capture zones result from the model insight that a successful reception does not only depends on the signal

power ratio between interfering signals but also on the time and phase offsets of sender and receiver.

Finally, to show the accuracy of our model, we implement and experiment with an application that is strongly dependent on the physical layer characteristics, the reception of unsynchronized signals. We perform this experiment with two widely used commercial IEEE 802.15.4 receiver implementations (TI CC2420 and Atmel AT86RF230) to demonstrate that our results are receiver-independent ($\rightarrow$ Section VI). The results validate our claim that our model accurately captures the behavior of realistic receivers in the face of concurrent transmissions.

Our implementation of the model and simulation code is available for download at http://disco.cs.uni-kl.de/content/collisions. There, the interested reader can also find an interactive visualization of the model for better comprehension of the bit errors in concurrent transmissions.

II. Factors to the Successful Reception of Concurrent Transmissions

Different factors impact the probability of successful reception under collisions. This section discusses the main factors that have been discussed in the literature. These factors will then be considered in our mathematical model that combines these factors to predict the success of concurrent transmissions.

Power ratio. The signal power is the most crucial factor for signal reception in general, and it also plays a major role in the reception of collisions. SINR-based models are widely used to model the packet reception in shared media, for example in the Physical Model [10] and its variants [2], [11]. The classical SINR model states that a stronger signal is received if its signal power exceeds the channel noise and the sum of interfering signals by a given threshold, i.e.,

$$\frac{P_s}{P_n + \sum P_i} > \delta_{\text{SINR}}. \tag{1}$$

This simple model is accurate for additive white Gaussian noise (AWGN) type of interference and independent payloads. However, when the sum of the interference is not AWGN such as for colliding packets or packets that are correlated, this model is not always accurate and other impact factors must be taken into consideration [9], [14], [23].

Signal timing. The relative timing of colliding packets greatly influences the outcome of the reception. This is because the receiver locks onto a packet during the synchronization phase at the start of a transmission, and if a stronger signal arrives later it disturbs the reception of the first packet and both packets in the collision are lost. Thus, in packet radio, capture alone is not sufficient for successful reception, rather the receiver must be synchronized and locked onto the captured signal as well. Several research contributions analyze possible collision constellations and their effect on packet reception [14], [23], and propose a new receiver design that releases the lock when a stronger packet arrives, discards the first and receives the second packet, the so-called *message-in-message (MIM) capture* [14], [28]. Subsequent work applies these insights to improve network throughput.

For example, Manweiler et al. [18] propose collisions scheduling to ensure that MIM is leveraged, thus increasing spatial reuse.

Channel coding. A further factor that influences packet reception success is bit-level coding. For example, in DSSS systems a group of b bits is mapped to a longer sequence of B chips [21]. The benefit of this approach is that resilience to interference is increased because the chipping sequences can be cross-correlated at the receiver, which effectively filters out uncoded noise. However, DSSS systems require interfering signals to be uncorrelated, e.g., ones not using coding or employing different chipping sequences (as in CDMA), to achieve their theoretical coding gain. Another possibility is a sufficient time offset of interfering packets with the same coding; this phenomenon is known as *delay capture* [4]. As networking standards such as IEEE 802.11 and IEEE 802.15.4 generally use DSSS with identical codes for all participants, existing experimental works on collisions and capture implicitly observe the effects of DSSS in such situations as well.

Packet contents. Experimental results show that the use of packets with identical payload and aligned starting times results in good reception performance and reduced latency in broadcast scenarios. For example, Dutta et al. [5] show that short packets can be received in such collisions with a PRR over 90 %, thus enabling the design of an efficient receiver-initiated link layer. Similarly, the latency in flooding algorithms widely used in WSNs can be greatly reduced [6], [27]. In these works experiments in IEEE 802.15.4 networks revealed that the tolerable time offset is very small (approx. 200 ns), which adds challenges to protocol design and implementation. These insights also show that capture and packet synchronization are not sufficient to explain these protocols' performance, bit-level modeling is necessary that includes both timing and content.

Carrier phase. Considering the reception of bits at the physical layer, the carrier phase of a signal is crucial for successful reception because the information is carried in the phase variations of the signal such that these offsets should be minimized [21]. Typically this is achieved during the synchronization phase of packet reception, and thus existing models chose to omit phase offsets. However, there are two reasons that this is not sufficient. First, in novel protocols exploiting packet collisions the synchronization during the preamble is not always able to succeed. Second, there are other novel applications that try to abandon the synchronization procedure. For example, Pöpper et al. [20] investigate the possibility of replacing individual message bits on the physical layer, and conclude that carrier phase offsets are the major hindrance to do so reliably.

III. System Model

In this section, we discuss the system model underlying our analysis, as shown in Fig. 1. From a bird's eye view, the model consists of three parts: *(i)* the sender model that modulates the physical layer signals of $n + 1$ transmitters, one fully synchronized signal of interest (SoI) and n interferers with possibly differing transmission starting times and payloads; *(ii)* the channel model with all senders sharing a single collision channel that outputs a scaled superposition of all signals (according to their corresponding power at the receiver), and *(iii)* the receiver model with three detection methods: uncoded, DSSS

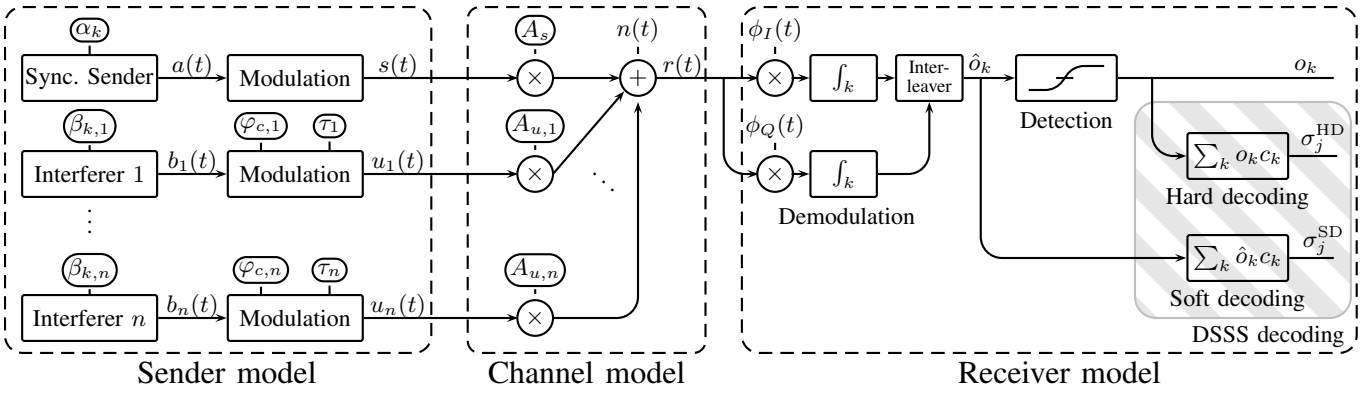


Figure 1. System model, its parameters are shown in ovals (payload bits α_k, β_k, carrier phase offset φ_c, time offset τ, signal amplitudes A_s, A_u). We consider one synchronized sender and n interferers on a collision channel that is the input to a receiver. There, three channel coding schemes are considered, *(i)* uncoded, *(ii)* DSSS with hard decision decoding (HDD) at the receiver, and *(iii)* soft decision decoding (SDD); resulting in different receiver paths.

with hard decision decoding (HDD), and DSSS with soft decision decoding (SDD). In the following, we discuss each component in detail. The notation used is collected in Table I.

A. Sender Model

In the first component, we modulate the physical layer signals of $n+1$ senders. We instantiate our model with the Minimum Shift Keying (MSK) modulation, a widely used digital modulation with desirable properties, and of special interest because of its use in the 2.4 GHz PHY of IEEE 802.15.4 [1, §6.5]. For the signal representations, we follow the notation of Proakis and Salehi [21, §4.3].

1) Synchronized sender: We assume that the receiver is fully synchronized to the SoI, i.e., the synchronization process has successfully acquired this signal and all interferers have relative offsets to it. The signal is then given by

$$s(t) = a_I(t)\cos\left(\frac{\pi t}{2T}\right)\cos\omega_c t + a_Q(t)\sin\left(\frac{\pi t}{2T}\right)\sin\omega_c t. \tag{2}$$

The signal consists of two components, the in- and the quadrature-phase component (I/Q). Modulated on each component are the information signals (carrying the bits represented by $\alpha_k^I, \alpha_k^Q \in \{\pm 1\}$) given by

$$\begin{aligned} a_I(t) &= \sum_{k=-\infty}^{\infty} \alpha_k^I \Pi\left(\frac{t-2kT}{2T}\right) \\ a_Q(t) &= \sum_{k=-\infty}^{\infty} \alpha_k^Q \Pi\left(\frac{t-(2k+1)T}{2T}\right), \end{aligned} \tag{3}$$

which represents a train of unit pulses Π with duration $2T$, the bit duration of the modulation (e.g., $2T = 1\,\mu$s in IEEE 802.15.4). The unit pulses are defined by

$$\Pi(t) = \begin{cases} 0 & \text{if } |t| > \frac{1}{2} \\ \frac{1}{2} & \text{if } |t| = \frac{1}{2} \\ 1 & \text{if } |t| < \frac{1}{2} \end{cases} \tag{4}$$

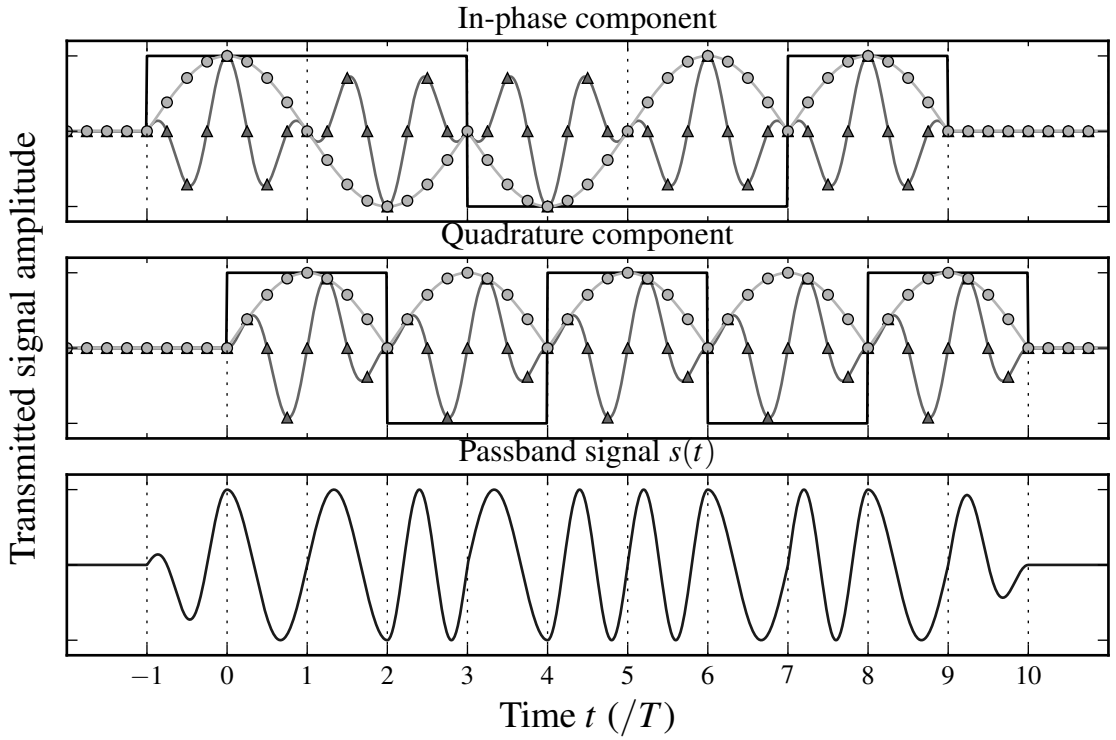


Figure 2. MSK modulation example. The modulated bit sequence is 1**1**0**0**1**0**0**1**1 (quadrature-phase bits are in boldface); it is multiplexed to the IQ components (blue rectangles), pulse-shaped with half-sines (red sinusoids with ∘ markers) and modulated on a carrier, resulting in the green waveform (with △ markers). Fir the quadrature component, we observe an additional staggering of T (MSK can be viewed as O-QPSK with half-sine pulse shaping). Both modulated IQ signals are added to result in the (real-valued) passband signal in the bottom figure.

The information signals are staggered, i.e., the Q-phase information signal is delayed by T. These signals are then shaped with half-sine pulses with duration $2T$, and modulated onto a carrier with frequency $\omega_c/2\pi$ (e.g., 2.4–2.48 GHz in IEEE 802.15.4). In the following, we use the angular frequency of baseband pulses $\omega_p = \pi/2T$, such that the first cosine term may be represented by $\cos \omega_p t$. A graphical illustration of such an MSK-modulated signal is shown in Fig. 2.

2) (Unsynchronized) interferers: In addition to the synchronized sender, we consider n interferers transmitting concurrently using the same modulation. These signals may not be synchronized to the receiver and each may carry its own payload. This introduces three additional parameters that influence the signal, the time offset τ_i, the carrier phase offset $\varphi_{c,i}$, and the information bits $\beta_{k,i}$. With a positive τ_i, an interferer starts its transmission later compared to the synchronized sender. The resulting signal for interferer i is given by

$$\begin{aligned} u_i\left(t;\tau_i,\varphi_{c,i}\right) = {} & b_{I,i}\left(t-\tau_i\right)\cos\omega_p\left(t-\tau_i\right)\cos\left(\omega_c t+\varphi_{c,i}\right) \\ & + b_{Q,i}\left(t-\tau_i\right)\sin\omega_p\left(t-\tau_i\right)\sin\left(\omega_c t+\varphi_{c,i}\right). \end{aligned} \tag{5}$$

We assume that the phase offsets $\varphi_{c,i}$ are constant for the duration of one packet, i.e., there is no carrier frequency offset during a transmission. In our experiments in Section VI, we show that this assumption is reasonable because receiver implementations are compensating

the drifts. For convenience, we express the pulse phase offset that is introduced by τ_i as $\varphi_{p,i} = \omega_p \tau_i$.

B. Channel Model

In our model, we use an additive collision channel. The relation for the output signal is

$$r(t) = A_s\, s(t) + \sum_{i=1}^{n} A_{u,i}\, u_i(t; \tau_i, \varphi_{c,i}) + n(t). \tag{6}$$

Each signal is scaled by a factor A_{x}, which contains both, possible signal amplifications by the sender and path loss effects that reduce the power at the receiver. In our evaluation, we use the Signal to Interference Ratio (SIR) at the receiver, given by

$$\mathrm{SIR} = \frac{A_s^2}{\sum_{i=1}^{n} A_{u,i}}, \tag{7}$$

to characterize the power relationship of the interfering signals. The contribution of all noise effects is cumulated in the linear noise term $n(t)$; possible instantiations are a noiseless channel or Gaussian noise.

C. Receiver Model

In the final component of the model, we feed the signals' superposition $r(t)$ into an optimal receiver to discern the detected bits. The signal is demodulated and fed into one of three detector implementations: one for uncoded bits, and two variants of DSSS decoding.

1) Demodulation: The signal demodulation step is performed for I and Q individually and the bits are then interleaved. We limit our discussion to the I component for brevity.

We use the matched filter function $\phi_I(t) = \cos\omega_p t \cos\omega_c t$ and low-pass filtering for downconversion and demodulation, which is the optimal receiver for noiseless and Gaussian channels [22]. It is multiplied with the received signal $r(t)$ and integrated for each bit period k to form the decision variable

$$\hat{o}_k^I = \Lambda_r^I(k) = \int_{(2k-1)T}^{(2k+1)T} r(t)\, \phi_I(t)\, dt. \tag{8}$$

The resulting value is called *soft bit*, with values $\hat{o}_k^I \in [-1, 1]$. Because the combination of the interferers in the received signal is linear the individual contributions can be divided into integrals for each signal:

$$\hat{o}_k^I = \Lambda_s^I(k) + \sum_{i=1}^{n} \Lambda_{u_i}^I(k) + \Lambda_n^I(k). \tag{9}$$

In our analytical evaluation in the next section, we derive closed-form expressions for the contributions $\Lambda_{u_i}^I$ and $\Lambda_{u_i}^Q$ to analyze the receiver output after a collision.

2) Uncoded bit detection: The detection operation for uncoded transmissions is slicing, essentially a sign operation on demodulation output, which results in the binary output $o_k \in \{\pm 1\}$. Thus, a bit of the SoI is flipped if the contribution from the interferers changes the bit's sign.

3) DSSS decoding: For coded transmissions, the number of chips exceeds the bits in a symbol, i.e., even if several chips are flipped it is still possible to decode a symbol correctly. There are 2^b symbols ξ with chipping sequences c_ξ, and B as the block length (i.e., the number of chips). For example, we have $b = 4$, $B = 32$ in IEEE 802.15.4.

We consider two modes of operation for the DSSS decoder, namely hard decision decoding (HDD) and soft decision decoding (SDD).

In *HDD*, the decoder uses sliced values o_k as its input, and then either chooses the symbol with the minimum Hamming distance or the one with the highest bit-wise cross-correlation to all chipping sequences. The decoder output is the symbol σ_j^{HD}, i.e., a group of b bits. For HDD, the decoder is given by

$$\sigma_j^{\mathrm{HD}} = \arg \max_{0 \le \xi < 2^b} \left| \sum_{k=0}^{B-1} o_{jB+k}\, c_{\xi,k} \right|. \tag{10}$$

In *SDD*, the demodulator output $\hat{o}_k$ is used directly as decoder input. This is beneficial because soft bits provide a measure of detection confidence. Apart from that, the operation is the same as for HDD with cross-correlation.

IV. Mathematical Analysis

Based on the system model in Fig. 1 we analyze the contributions of each interfering signal to the overall demodulator output; the sum of these contributions is the decision variable of bit detection. We first present the most general case considering all system parameters in Theorem 1. Subsequently, we illustrate its interpretation in selected parameter combinations.

Theorem 1. *For an interfering MSK signal $u(t)$ with parameters τ and φ_c, the contribution to the demodulation output $\Lambda_u^I(k)$ is given by Eq. (14) in Table II.*[1]

Due to space restrictions, the proof of this theorem can be found in Appendix B. To provide a better understanding of the effects of the parameters, we focus on selected parameters and discuss the resulting equations. Then we revisit Theorem 1 and discuss the combination of effects.

1) Synchronized signal: In the simplest case both offsets, time and phase, are zero, i.e., the signal is fully synchronized to the receiver. The result is given in Eq. (11). The signal's contribution to the k-th bit is $\Lambda_u(k) = \frac{T}{2} A_u \beta_k$. The bit decision of bit k, i.e., the sign of the equation, is governed by β_k. The magnitude of the contribution is controlled by the amplitude of the signal A_u, and thus stronger signals lead to a greater contribution to the decision variable $\hat{o}_k$. As an example, consider two signals $s(t)$ and $u(t)$ that are both fully synchronized to the receiver. The output of the demodulator of bit k is

[1]We omit the subscript i for clarity in the equations. The results for the quadrature phase are given by the same equations when the roles of I and Q are interchanged.

Symbol	Definition
$s(t)$	MSK signal by the synchronized sender as defined in Eq. (2)
$u_i(t)$	MSK signal by interferer i, with possible offsets τ_i and $\varphi_{c,i}$ (Eq. (5))
$r\,(t)$	Resulting superposition of signals at the receiver (Eq. (6))
$2T$	Bit duration, e.g., $2T = 1\,\mu$s in IEEE 802.15.4
$\omega_c = 2\pi f_c$	Angular speed of the carrier wave with frequency f_c
$\omega_p = \frac{\pi}{2T}$	Angular speed of baseband pulses (periodic by $4T$)
τ_i	Time offset (positive shifts denote a starting delay)
$\varphi_{c,i}$	Carrier phase offset in the passband of interferer i
$\varphi_{p,i} = \omega_p \tau_i$	Baseband pulse phase offset of interferer i, equivalent to time offset
$A_{s,} A_{u_i}$	Signal amplitudes of $s\,(t)$, $u_i\,(t)$ at the receiver
$\Pi\,(t)$	Unit pulse (step) function as defined in Eq. (4)
$a_I, a_Q\,(t)$; $b_{I,} b_Q\,(t)$	Information sequences consisting of unit pulses $\Pi(t)$ (Eq. (3))
α_k^I, α_k^Q; β_k^I, β_k^Q	Information bit k of the synchronized sender and interferers
$\phi_I, \phi_Q\,(t)$	Basis function of the MSK modulation to demodulate bits
$\Lambda_u\,(k)$	Contribution of signal $u\,(t)$ to the bit decision in bit interval k (Eq. (8))
$\hat{o}_k^I$	Decision variable of the detector for bit k of I component
o_k^I	Detected bit of an uncoded transmission
ξ	Input symbol at the sender
$c_{\xi,k}$	Chipping sequence of symbol ξ (see also Table III)
$\sigma_j^{HD}, \sigma_j^{SD}$	Detected symbol after DSSS decoding, the index j compensates that each symbol consists of 16 IQ pairs (see Eq. (10))
$k' = k - \lfloor \tau/2T \rfloor$	Correction factor for the bits active in a decision interval
$\underline{\tau} = \tau - 2k'T$	Relative shift in a bit of interest k
$k^{Q\prime} = k - \lfloor (\tau + T)/2T \rfloor$	Correction factor for Q bits during I detection
$k^{I\prime} = k - \lfloor (\tau - T)/2T \rfloor$	Correction factor for I bits during Q detection
$\underline{\tau^Q} = \tau + T - 2k^{Q\prime}T$	Relative shift in a bit of interest k for the leaking Q-phase
$\underline{\tau^I} = \tau - T - 2k^{I\prime}T$	Relative shift in a bit of interest k for the leaking I-phase

Table I
NOTATION USED IN THE DERIVATIONS.

No offsets

$$\Lambda_u^I\,(k) = \tfrac{T}{2} A_u \beta_k^I \tag{11}$$

Carrier phase offset φ_c

$$\Lambda_u^I\,(k) = \tfrac{T}{2} A_u \left(\cos\varphi_c \beta_k^I - \tfrac{1}{\pi} \sin\varphi_c \left(\beta_{k-1}^Q - \beta_k^Q \right) \right) \tag{12}$$

Time offset τ

$$\Lambda_u^I\,(k) = \tfrac{1}{4} A_u \left[\cos\varphi_p \left(\underline{\tau} \beta_{k'-1}^I + (2T - \underline{\tau})\,\beta_{k'}^I \right) - \tfrac{2T}{\pi} \sin\varphi_p \left(\beta_{k'-1}^I - \beta_{k'}^I \right) \right] \tag{13}$$

Carrier phase + time offset

$$\begin{aligned} \Lambda_u^I\,(k) = \tfrac{1}{4} A_u \Big\{ & \cos\varphi_c \left[\cos\varphi_p \left(\underline{\tau} \beta_{k'-1}^I + (2T - \underline{\tau})\,\beta_{k'}^I \right) - \tfrac{2T}{\pi} \sin\varphi_p \left(\beta_{k'-1}^I - \beta_{k'}^I \right) \right] \\ & - \sin\varphi_c \left[\sin\varphi_p \left(\underline{\tau^Q} \beta_{k^{Q\prime}-1}^Q + \left(2T - \underline{\tau^Q}\right) \beta_{k^{Q\prime}}^Q \right) + \tfrac{2T}{\pi} \cos\varphi_p \left(\beta_{k^{Q\prime}-1}^Q - \beta_{k^{Q\prime}}^Q \right) \right] \Big\} \end{aligned} \tag{14}$$

Table II
ANALYTICAL RESULTS: CONTRIBUTIONS OF AN INTERFERING SIGNAL TO THE DEMODULATOR OUTPUT.

then $\frac{T}{2}\left(A_s\alpha_k + A_u\beta_k\right)$. If both senders transmit the same bit ($\alpha_k = \beta_k$), then the signals interfere constructively and push the decision variable further away from zero. If on the other hand the bits are different, then the decision variable has the sign of the stronger signal; this is the well-known capture effect for a single bit.

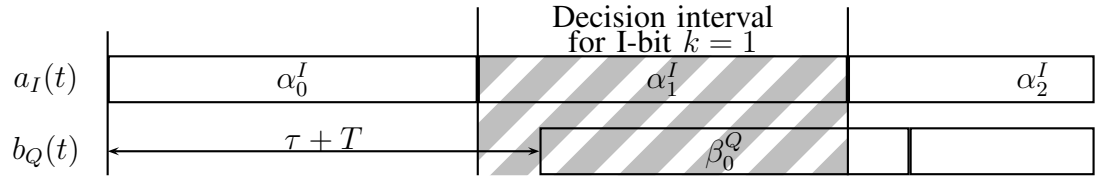


Figure 3. Carrier phase offset φ_c: several bits influence the bit decision on bit k in a collision between two signals. The carrier phase offsets lead to a leakage of the quadrature phase, and because the Q-bits are staggered, there is an additional shift of T in the bit indices. The active bits in the decision interval are highlighted.

2) Carrier phase offset: Next, we analyze the effect of carrier phase offsets when the signals are fully time-synchronized ($\tau = 0$). The result is given by Eq. (12). We observe two effects from carrier phase offset. First, the bit contribution of β_k is scaled by $\cos\varphi_c \leq 1$, which leads to reduced absolute values (and thus a smaller contribution to the decision variable) and potentially causes the bit β_k to flip for $\varphi_c \in \left(\frac{\pi}{2}, \frac{3\pi}{2}\right)$. Second, the quadrature phase starts to leak into the decision variable and thus two additional bits β_{k-1}^Q, β_k^Q that influence the outcome are present. This contribution, however, is scaled by $\pi^{-1}\sin\varphi_c$, and only appears when the two Q bits are alternating during the integration interval. In essence carrier phase offsets may lead to unpredictable bits in the detector output because of carrier phase offset induced bit flips.

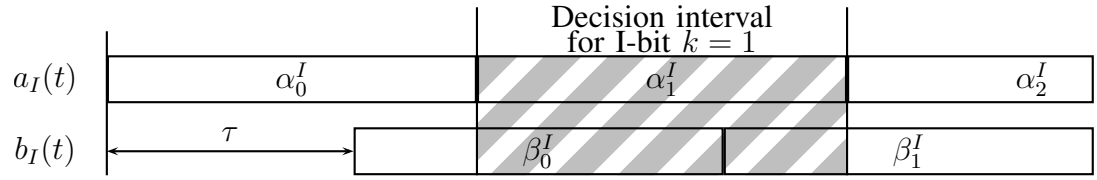


Figure 4. Time offset τ: several bits influence the bit decision on bit k in a collision between two signals. The active bits in the decision interval are highlighted.

3) Time offset: If the signal is phase-matched but relatively shifted in time, the demodulator output is given by Eq. (13). We make three observations here. The bit index k needs to be adjusted because bits may be time-shifted into the integration interval, see Fig. 4; the new index is given by $k' = k - \lfloor \tau/2T \rfloor$. We call these *active bits* because they contribute to the output. These bits overlap partially or fully, and their active time duration is $\underline{\tau} = \tau - 2\lfloor \tau/2T \rfloor T$ with values in $[0; 2T)$. However, these bits do not contribute to the decision directly but are multiplied with $\cos\varphi_p$. This means that bit contributions are diminished and can be flipped by time offsets. Finally, a term scaled by π^{-1} is introduced that is only present when bits are alternating. However, these bits are the same active bits as above, the Q phase does not leak in this setting.

4) Both offsets: Finally, when both offsets are present as in Theorem 1, we can interpret the result as a combination of the above effects. A graphical illustration of the active bits is shown in Fig. 5. Due to the staggering of bits (the Q bits are delayed by T),

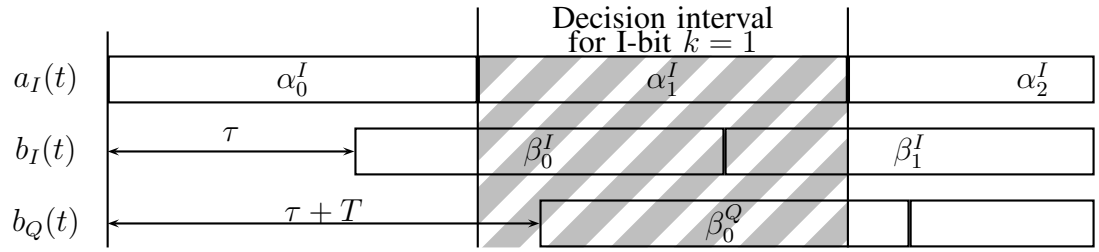


Figure 5. Time and phase offsets combined: the decision on bit k is influenced by up to five bits, one from the synchronized and four from the interfering signal.

the indices of leaking bits of the Q phase also need to be adjusted, the new index is $k^{Q\prime} = k - \lfloor (\tau + T)/2T \rfloor$, and the active time interval $\underline{\tau^Q}$ is derived similarly as above.

In summary, we observe that the contribution of the interfering signal is complex and that φ_c and φ_p can potentially flip the original bits β_k. As we will see in the next section, this should be bad news for collision-aware protocols that use identical payload to achieve constructive interference (e.g., [27]): these bits can flip easily and then generate destructive interference. However, the use of coding helps to alleviate these negative effects as we will see in the next section.

V. Parameter Space Exploration

Equipped with the closed-form analytical model of the bit-wise receiver outputs, we systematically explore the parameter space in detail.

A. Methodology

We perform Monte Carlo simulations across the full range of free model parameters to analyze the behavior of network performance metrics. We instantiate the model with the following parameter choices for sender and channel.

1) Sender model: To keep the evaluation tractable, we consider the presence of one synchronized sender and one interferer; we denote these parties as $\mathcal{S}$ and $\mathcal{I}$ with signals $s(t)$ and $u(t)$, respectively. We analyze the reception performance of groups of associated bits, or packets; in this case, a single bit error leads to a packet drop. The packet reception rate (PRR) is the fraction of packets that arrive without errors divided by the total number of packets. We use packets with a length of 64 bit. We consider two categories of colliding packets, either with independent ($\mathcal{S}$ and $\mathcal{I}$ trying to exploit spatial reuse) or identical content ($\alpha_k = \beta_k$, as it is the case for collision-aware flooding protocols). The bits to send are chosen in the following manner: for uncoded transmissions, α_k is drawn bitwise i.i.d. from a Bernoulli distribution over $\{-1, 1\}$, and either the same procedure is performed for β_k (independent packets) or simply copied over from α_k (identical packets). For coded packets, we draw symbols i.i.d. uniform random from $\{0, \ldots, 15\}$ and spread these symbols according to the chipping sequences defined by the IEEE 802.15.4 standard [1, §6.5]. This means that 4 bit groups are first spread to 32 bit chipping sequences before they are transmitted in α_k, β_k. The chipping sequences are given in Table III. Note that

Symbol ξ	Bits	Chipping sequence bits[ab] $(c_{\xi,0}, \ldots, c_{\xi,31})$																													
0	0000	**1**	**1**	**0**	**1**	1	0	0	1	1	1	0	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0	1	0	1	1	1	0
1	0001	1	1	1	0	**1**	**1**	**0**	**1**	1	0	0	1	1	1	0	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0	1	0
2	0010	0	0	1	0	1	1	1	0	**1**	**1**	**0**	**1**	1	0	0	1	1	1	0	0	0	0	1	1	0	1	0	1	0	0	1	0
3	0011	0	0	1	0	0	0	1	0	1	1	1	0	**1**	**1**	**0**	**1**	1	0	0	1	1	1	0	0	0	0	1	1	0	1	0	1
4	0100	0	1	0	1	0	0	1	0	0	0	1	0	1	1	1	0	**1**	**1**	**0**	**1**	1	0	0	1	1	1	0	0	0	0	1	1
5	0101	0	0	1	1	0	1	0	1	0	0	1	0	0	0	1	0	1	1	1	0	**1**	**1**	**0**	**1**	1	0	0	1	1	1	0	0
6	0110	1	1	0	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0	1	0	1	1	1	0	**1**	**1**	**0**	**1**	1	0	0	1
7	0111	1	0	0	1	1	1	0	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0	1	0	1	1	1	0	**1**	**1**	**0**	**1**
8[c]	1000	**1**	**0**	**0**	**0**	1	1	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	1	1	1	0	1	1	1	1	0	1	1
9	1001	1	0	1	1	**1**	**0**	**0**	**0**	1	1	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	1	1	1	0	1	1	1
10	1010	0	1	1	1	1	0	1	1	**1**	**0**	**0**	**0**	1	1	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	1	1	1
11	1011	0	1	1	1	0	1	1	1	1	0	1	1	**1**	**0**	**0**	**0**	1	1	0	0	1	0	0	1	0	1	1	0	0	0	0	0
12	1100	0	0	0	0	0	1	1	1	0	1	1	1	1	0	1	1	**1**	**0**	**0**	**0**	1	1	0	0	1	0	0	1	0	1	1	0
13	1101	0	1	1	0	0	0	0	0	0	1	1	1	0	1	1	1	1	0	1	1	**1**	**0**	**0**	**0**	1	1	0	0	1	0	0	1
14	1110	1	0	0	1	0	1	1	0	0	0	0	0	0	1	1	1	0	1	1	1	1	0	1	1	**1**	**0**	**0**	**0**	1	1	0	0
15	1111	1	1	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	1	1	1	0	1	1	1	1	0	1	1	**1**	**0**	**0**	**0**

[a]The IQ chips are shown interleaved, dark background denotes in-phase chips.
[b]The sequences are shifted cyclically by four chips, **bold chips** are the first chips of symbol 0 (or 8) for reference.
[c]The second half of the chipping sequences are equal to the first except that quadrature bits are inverted.

Table III
CHIPPING SEQUENCES USED IN THE 2.4 GHZ PHY OF IEEE 802.15.4.

for symbols `1`–`7`, the chipping sequences are shifted versions of the symbol `0`, while for the other half (symbols `8`–`15`), the quadrature-phase bits are inverted.

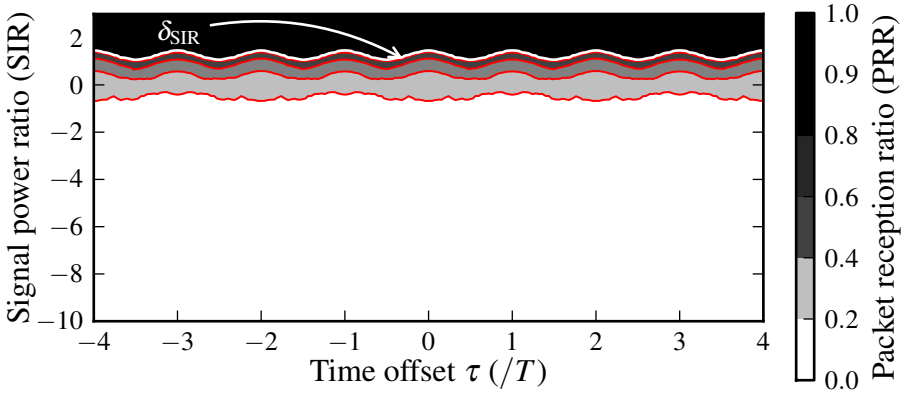
In accordance to the literature [22], as the carrier phase offset is hard to control because of oscillators drifts and other phase changes during transmission, we draw φ_c i.i.d. uniform randomly from $[0; 2\pi)$ for each packet in most settings. On the other hand, we use the same time offset τ for all packets because experimental work shows that this timing can be precisely controlled. We used 1,000 packets in our simulations.

2) Channel model: To highlight the impact of signal interference we consider a noiseless channel. This is a well-accepted assumption when both signals are significantly above noise floor level [19, §8]. We set $A_s = 1$ and $A_u = \mathrm{SIR}^{-\frac{1}{2}}$.

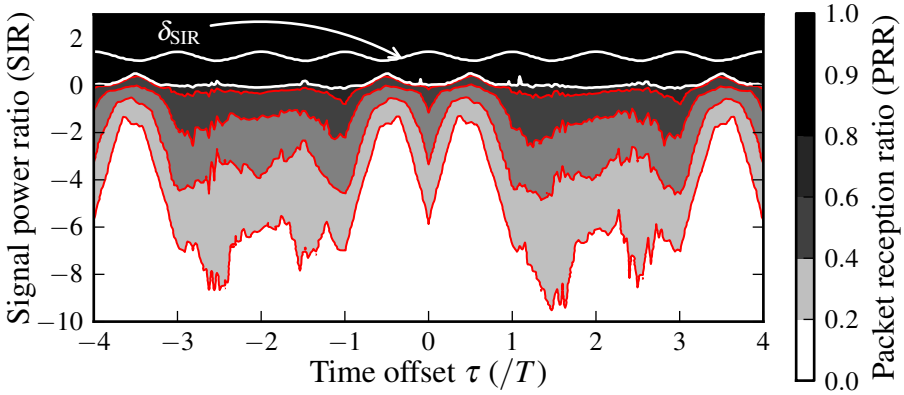
B. Reception of the Synchronized Signal of Interest

1) Capture threshold under independent payload: In our first case study, we consider the transmission of independent payload. This situation occurs, e.g., when two uncoordinated senders detect a clear channel, transmit, and the packets collide at the receiver. The metric of interest is the PRR of the SoI; and because we consider signals that are well above the noise floor (and thus reception is guaranteed without interferers), the PRR represents the probability of a receiver to overcome collisions. The results for three classes of receivers are shown in Fig. 6 and Fig. 7.

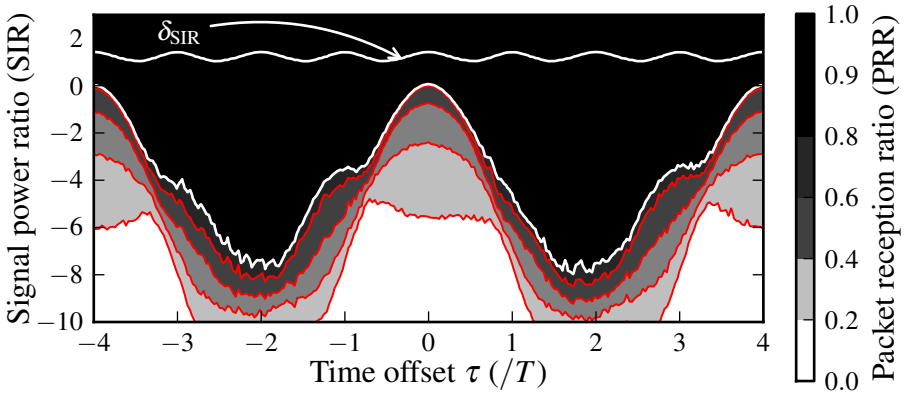
Uncoded transmissions. From Fig. 6a, we observe that the capture threshold is a good model to describe the PRR of interfering, uncoded transmissions. If the SoI is stronger



(a) Uncoded transmissions.

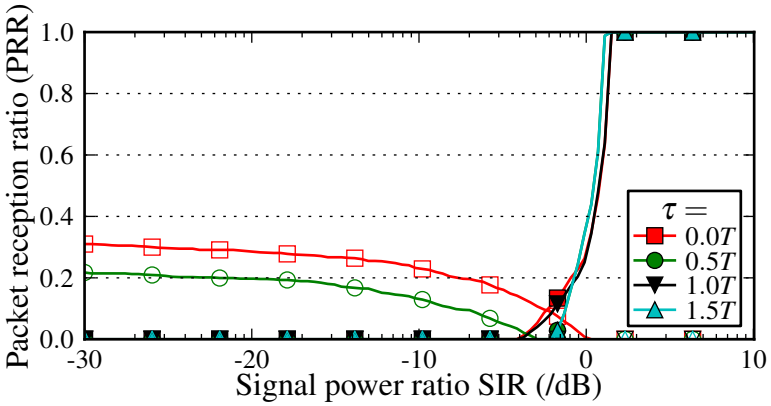


(b) DSSS with hard decision decoding (HDD).

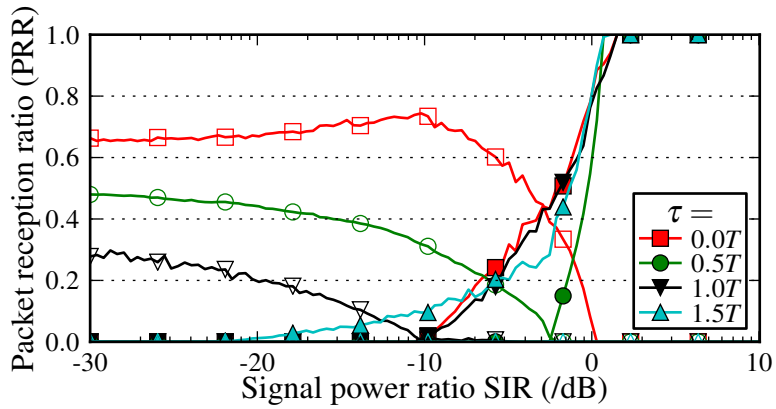


(c) DSSS with soft decision decoding (SDD).

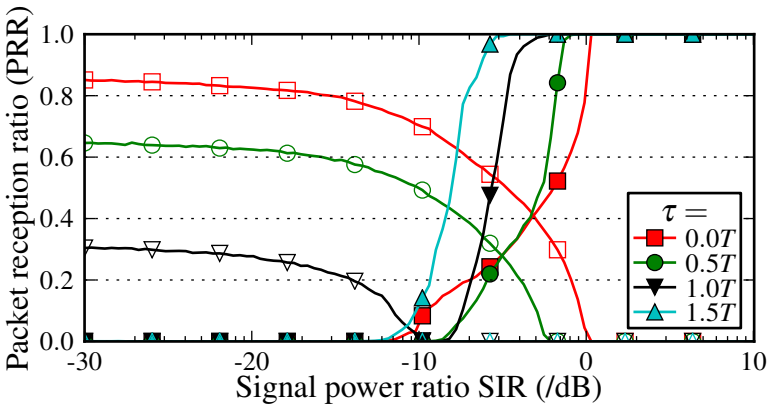
Figure 6. The capture threshold for two colliding packets with *independent* payload, depending on the signals' power ratio SIR and time offset ($\tau = 0$ indicates that the signals overlap perfectly). For the uncoded case, the threshold δ_{SIR} is nearly constant across all time offsets and represents the classical capture threshold (thus, for reference, it is drawn in all figures). For HDD, the threshold is nearly constant, but 1 dB lower. Additionally there is a wide transitional region with non-zero reception rates. Finally, for SDD the threshold is very sensitive to signal timing, we observe a possible gain of 8 dB with periodical time shifts of $2T$.



(a) Uncoded transmissions.



(b) DSSS with hard decision decoding (HDD).



(c) DSSS with soft decision decoding (SDD).

Figure 7. Effect of signal to interference power radio SIR to the PRR for *independent* payload.

by a threshold δ_{SIR} of 2 dB, all its packets are received. This behavior persists for all choices of τ, i.e., packet reception is independent from the properties of the interfering signal (we only see a minor periodic timing effect). Below the threshold, there is a narrow transitional region with non-zero PRR. Under uncoded transmissions, our model is able to recover the classical capture effect for the MSK modulation and is in accordance to experimental results in the literature [8], [25].

Hard decision decoding. When considering HDD (Fig. 6b), we note that the threshold abstraction is still valid and the performance improvement of coding is only 1 dB (the coding gain is canceled when the same chipping sequences are used). In the transitional region there is a wider range of parameter settings that result in non-zero PRRs, e.g., if τ is close to integer values (and thus $\cos\varphi_p \approx 0$), we observe a better PRR for $\mathcal{S}$. These results show that coding with HDD yields only limited benefits when all senders use identical chipping sequences.

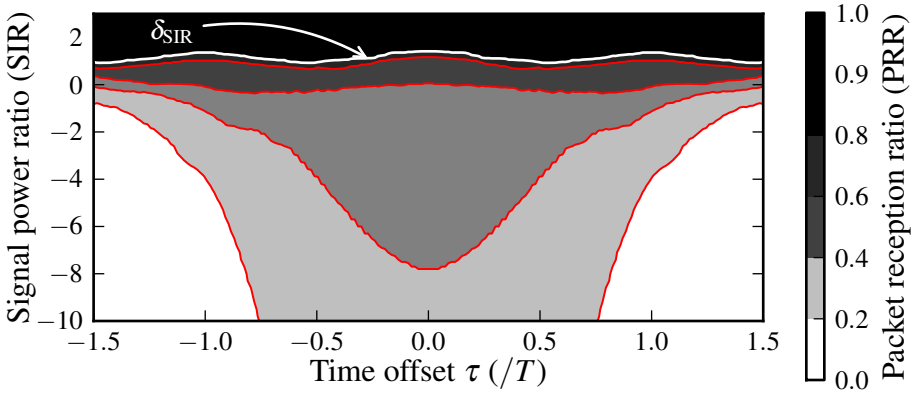
Soft decision decoding. Finally, for SDD we observe a strong dependence of PRR and time offset (Fig. 6c). Only for positions without chipping sequence shifts ($\tau = 0$, and because of the way IEEE 802.15.4 sequences are chosen[2] $\tau = 4kT$, $k \in \mathbb{Z}$) the performance is comparable to the HDD case; for different shifts, we can achieve a 6–8 dB coding gain despite the use of identical chipping sequences. Especially for offsets $\tau = 4kT + 2T$, we can achieve a clear coding gain. The reason is that soft bits contain additional information on the detection confidence, which helps to improve detection performance.

This insight suggests that two senders benefit from coding even when using identical sequences, provided that they time their collisions precisely. This may help to increase the number of opportunities for concurrent transmissions, i.e., interfering nodes can be much closer to a receiver with the same PRR performance. In other words, a *constant* capture threshold is too conservative when collision timing can be controlled, because then the performance of SDD is very sensitive to time offsets.

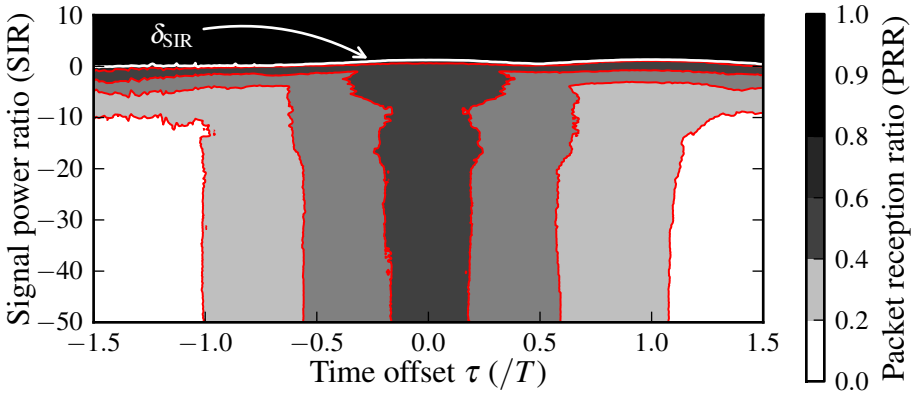
2) Capture threshold under identical payload: When considering the collisions of packets with identical payload, we observe very different results (Fig. 8 and Fig. 9): we see that good reception performance is possible despite a negative SIR.

Uncoded transmissions. For uncoded transmissions, the PRR performance is shown in Fig. 8a. While in this case the threshold for a PRR of 100 % is still equal to the independent payload case, substantially more packets are received in the transitional region with time shifts less than $\pm 0.75T$. However, PRRs around 30 % are usually not sufficient to boost the performance of network protocols. The reason for this low performance is the carrier phase offset φ_c: with low SIR, the interfering signal dominates the bit decision at the receiver, and with larger offsets $\varphi_c \in (\pi; 2\pi)$, the term $\cos\varphi_c$ changes its sign and flips all subsequent bits. In this sense, the literature conjecture that constructive interference is the reason for the good performance of flooding protocols [27] is only valid if the receiver is synchronized to the strongest signal and if the phase offset φ_c can be neglected. However, since packet preambles collide in the novel collision-aware protocols successful

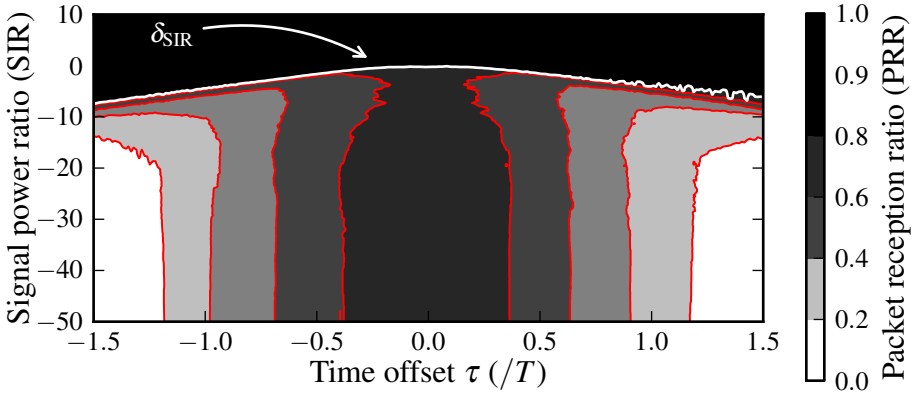
[2]See Table III. The chipping sequences are not independently chosen, they constitute shifted versions of a single generator sequence with shifts of 4 IQ bits.



(a) Uncoded transmissions.

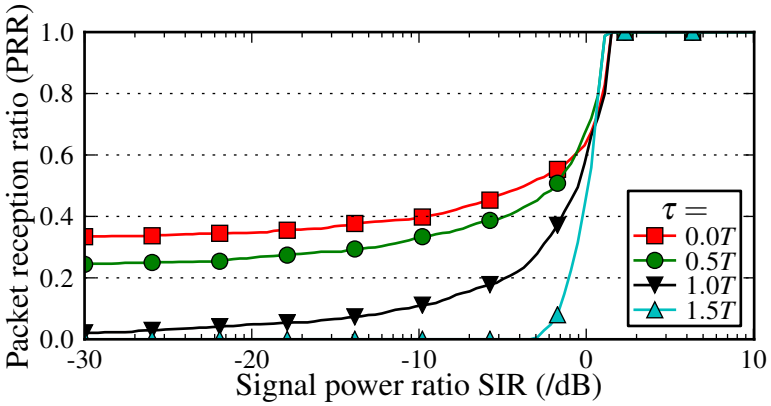


(b) DSSS with hard decision decoding.

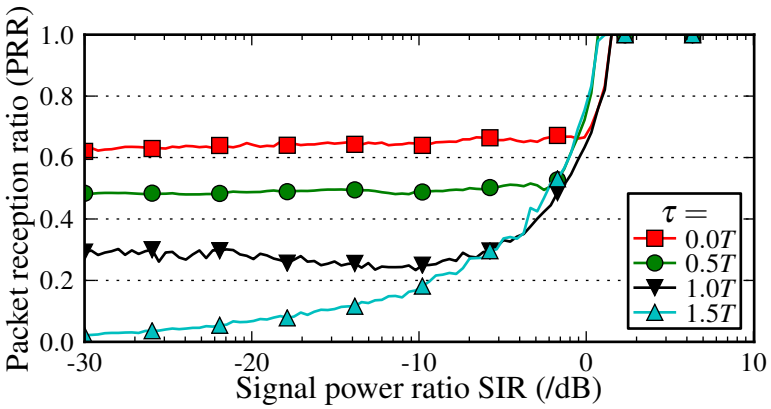


(c) DSSS with soft decision decoding.

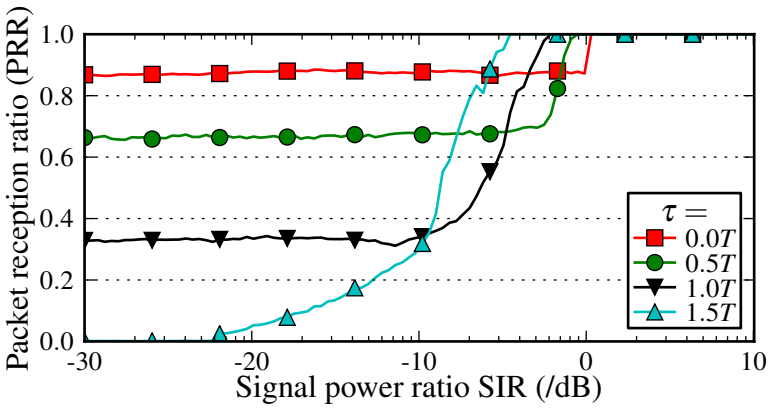
Figure 8. The capture threshold for colliding packets with *identical* content depending on the power ratio SIR and the time offset τ. In all three figures we show the threshold δ_{SIR} for identical and uncoded payload for reference. (a) In the uncoded case, the PRR is non-zero in the transitional range, but packet loss is still likely with PRRs of 20–30 %. For coded transmissions, we observe a central area that enables high PRR values (up to 70 % in (b) and over 90 % in (c)).



(a) Uncoded transmissions.



(b) DSSS with hard decision decoding (HDD).



(c) DSSS with soft decision decoding (SDD).

Figure 9. Effect of signal to interference power radio SIR to the PRR for *identical* payload.

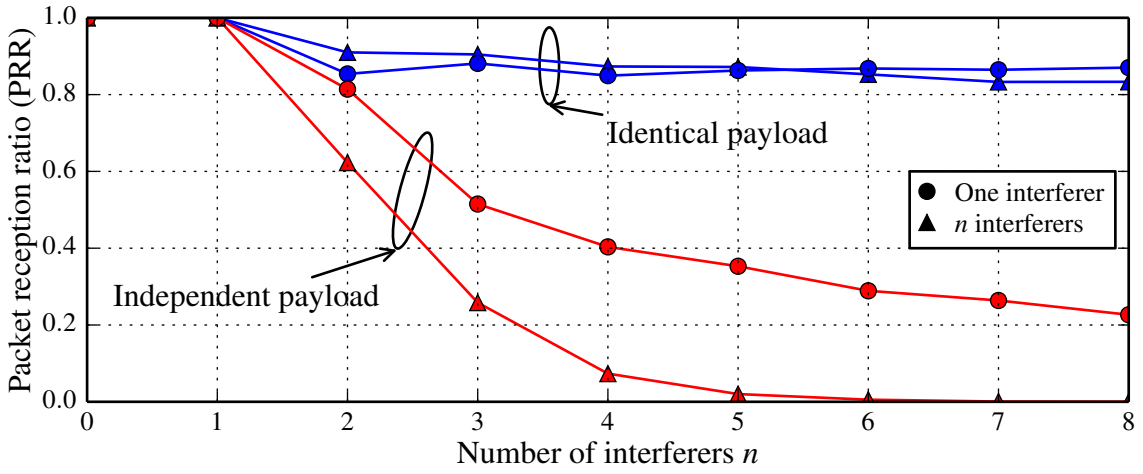


Figure 10. Reception ratio for SDD under one strong interferer or n weaker interferers, but both with equal signal power at the receiver. For identical payload the difference is small, for independent payload several interferers are more destructive than one.

synchronization cannot be ensured, and there must be other mechanisms to overcome phase-induced bit flipping.

Hard decision decoding. The reception performance of coded messages provides a hint in this direction (Fig. 8b). We observe a corridor of τ values ($\tau = \pm 0.2T$ or 100 ns in IEEE 802.15.4) that has a PRR of 60–80 % in the center (note the larger SIR scale on the y-axis). When two signals with identical payload collide with small time shifts, a reception is still possible, even if the interfering signal is far stronger. This suggests that the interfering signal is received instead of the SoI, and that coding helps to overcome bit flips of β_k induced by the carrier phase. The explanation is a property of Eq. (10): even if all bits are flipped by $\cos\varphi_c$, the (absolute) correlation is still maximal for the correct chipping sequence. This shows that the coding used in IEEE 802.15.4 is a key factor to make the novel collision-aware protocols work.

Soft decision decoding. The experimentally observed performance in the literature is even superior to Fig. 8b [5], [6], [27]. Taking SDD into account, this gap is closed (Fig. 8c). There is a strong center region for $\tau \leq \pm 0.3T$, or 150 ns in 802.15.4, with a PRR of over 90 %. Now, this is in good match to the existing experimental results. This means that the reception performance is very good in this center region *independent* of the SIR, i.e., no power control is required and perfect time synchronization is unnecessary for successful reception.

3) Effect of Several Interferers: In this subsection we consider the effect of one strong interferer compared to several interferers with the same power when combined, but evenly distributed across the interferers. We consider the following scenario: all interferers are time-synchronized ($\tau_i = 0$), but each has an i.i.d. uniform random phase offset $\varphi_{c,i}$ (and independent payload bits $\beta_{k,i}$ if different content is assumed). The interference power varies with $\frac{n}{2}P_{\mathrm{SoI}}$ for a number of interferers $n \in \{1, \ldots, 8\}$, with each interferer having a signal power at the receiver of $\frac{1}{2}P_{\mathrm{SoI}}$.

Under the classical capture threshold model both interference types share the same SIR and thus lead to the same PRR at the receiver. However, as we observe in Fig. 10, this is only the case for identical payload, for independent payload n interferers prove to be more destructive despite having the same signal power. While experimental results by Ferrari et al. suggested this result [6, Fig. 12] for identical payload, the root cause is now explained by our model. The observation for independent payload reveals another problem of SINR models: relying on the signal power ratio alone discards the crucial effects of each interferer's offsets.

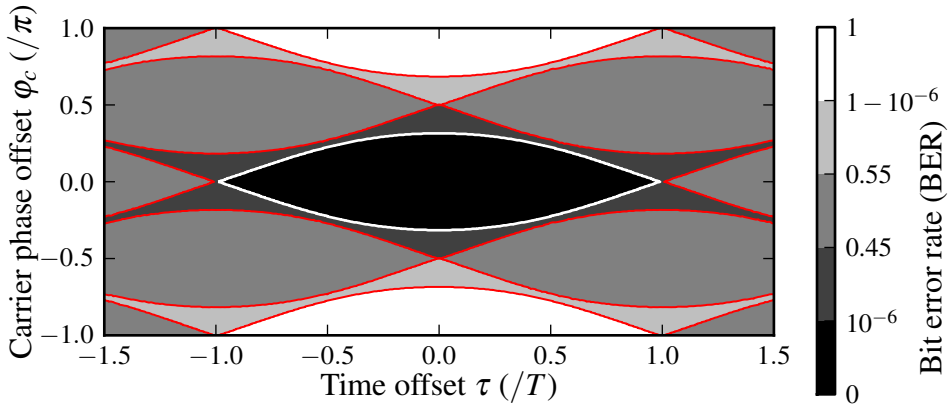
C. Reception of Interfering Signals with Independent Payload

Our results explain why and when collision-aware protocols work: coding enables the reception of interfering signals despite signal phase and time offsets. In this section, we revisit the case of independent payload but focus our interest now on the reception of the *interfering* signal, i.e., we treat the interfering signal $u\left(t\right)$ as the SoI and observe the reception of β_k instead of α_k. Related work by Pöpper et al. [20] shows that for uncoded systems the reception of interfering signals is indeterministic; in contrast, we show analytically and experimentally (Section VI) that real systems can receive interfering packets reliably when using *coded* messages.

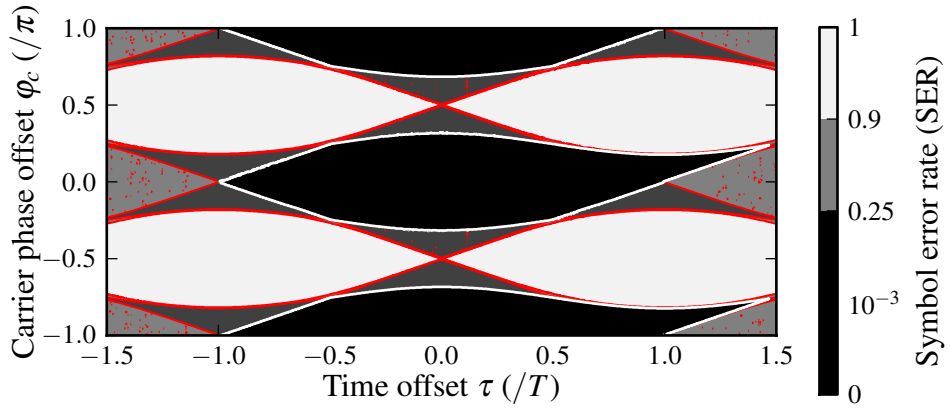
Uncoded transmissions. This case is shown in Fig. 12a. In this case a reception is only successful if bits are not flipped by φ_c or φ_p, and in our evaluation we observe a PRR of 20–30 % in the center region ($\mathrm{SIR} < -10\,\mathrm{dB}$ and $|\tau| < 0.5T$). The reason why the reception performance is so low is visible in Fig. 11a; the acceptable parameter values of τ and φ_c that lead to a error-free packet reception have tight constraints. The interfering signal must hit into a *capture zone* defined by the signal parameters.

Hard decision decoding. In this setting the PRR in the central area rises to approx. 60 % (Fig. 12b). In Fig. 11b we see the reason for the increase: while the general shape is the same, we see a second capture zone around $\varphi_c = \pm\pi$. There are two explanations for this. First, we use the same sliced bits from the uncoded case as input for DSSS correlation, which thus possess the same error characteristics. Second, because of the use of absolute correlation values in the correlation (Eq. (10)), the adverse effect of large phase offsets can be repaired. The use of DSSS with absolute correlation thus doubles the PRR under an interfering signal.

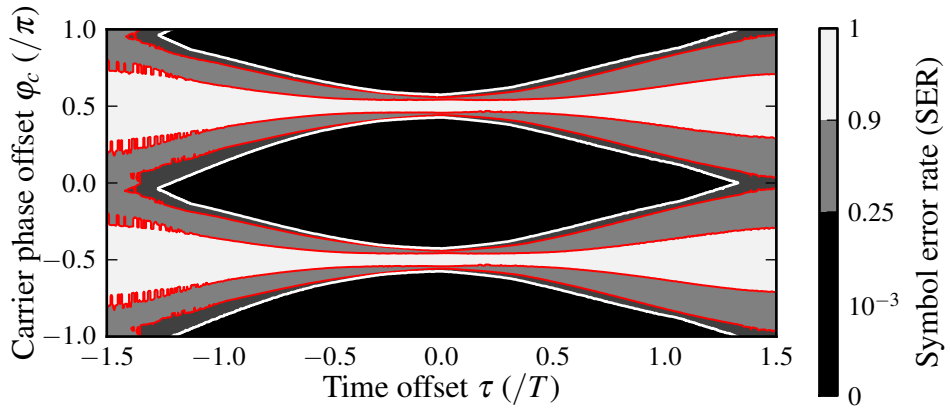
Soft decision decoding. Finally, in Fig. 12c we see a central area below $\mathrm{SIR} = -23\,\mathrm{dB}$ and a width of $0.2T$ that has a PRR for the interfering signal over 90 %. This means that, if the power difference is large enough, a receiver can ignore a synchronized signal and recover the interfering one despite its offsets. Fig. 11c shows this in terms of the capture zone. The eye-shaped regions are much wider compared to the other receiver designs, and especially for the central region with minor deviations of τ, the symbol error rate is negligible. Problems in the reception only occur for carrier phase offsets such that $\cos\varphi_c \approx 0$. These results show that interfering signals can indeed be received, which helps in collision-aware protocols or other intentional collisions, e.g., in message manipulation attacks on the physical layer. To validate this new result, we present an experimental study of such reception with real receiver implementations next.



(a) Bit error rate for uncoded transmissions.

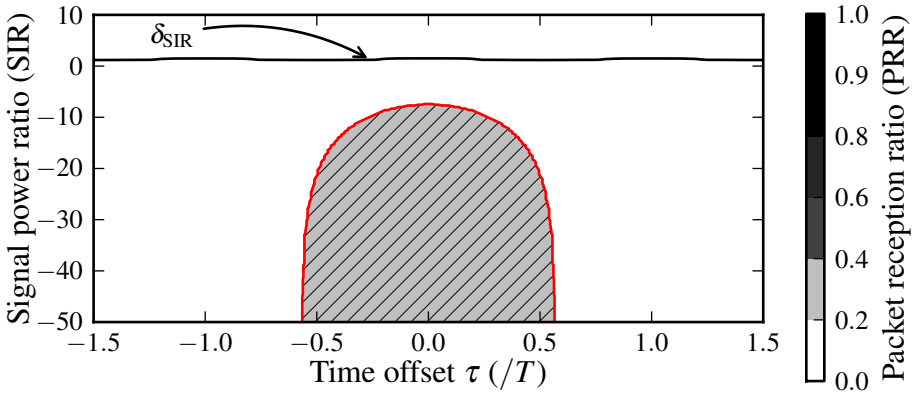


(b) Symbol error rate for DSSS with hard decision decoding (HDD).

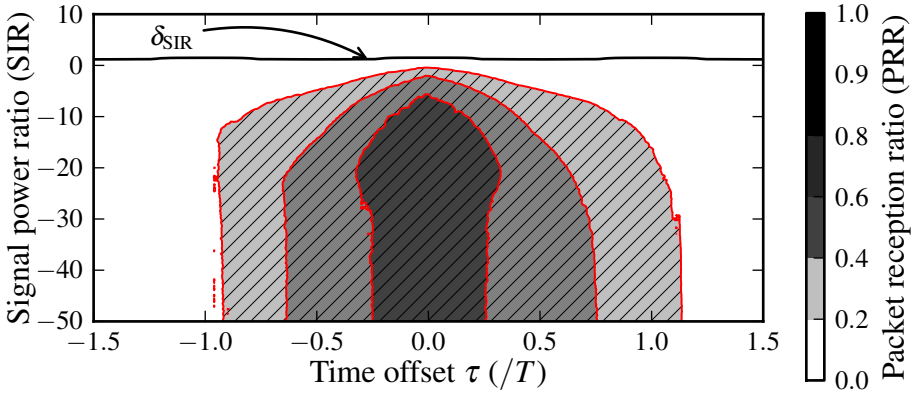


(c) Symbol error rate for DSSS and soft decision decoding (SDD).

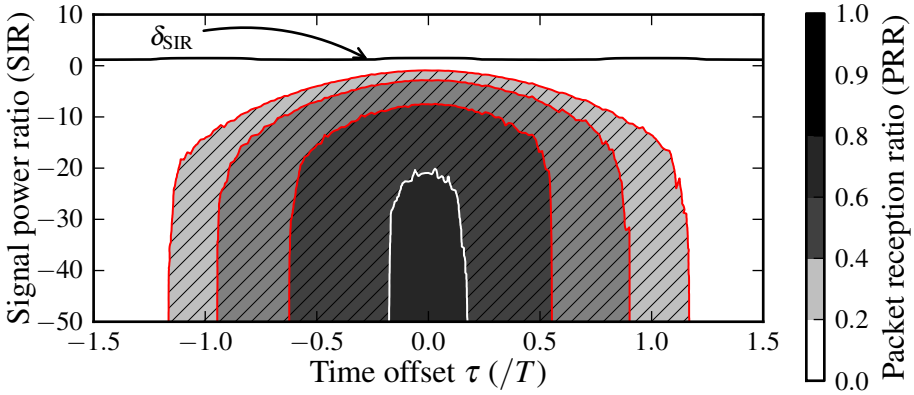
Figure 11. Relation between error rates and signal parameters, time offset τ and carrier phase offset φ_c. A packet is successfully received if the parameter combinations fall inside the dark *capture zones*. (a) For uncoded transmissions, the error rate increases for phase offsets $|\varphi_c| > \frac{\pi}{4}$. (b) For coded transmissions and a HDD receiver, the shape of the capture zone is similar to the case in (a), but a second zone around $\varphi_c = \pi$ is present. (c) For coded transmission and SDD, the eye shape is widened, and an increasing number of parameter combinations result in error-free transmissions.



(a) Uncoded transmissions.

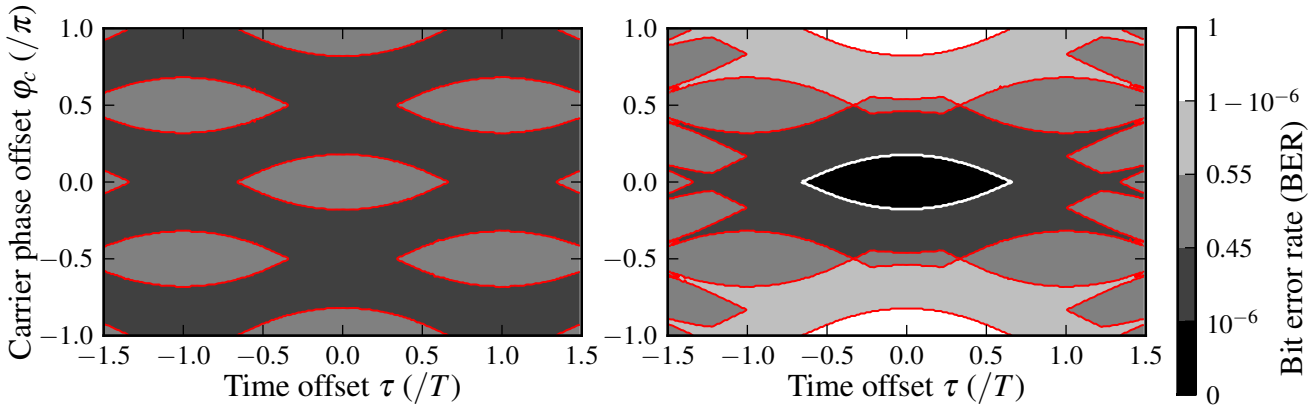


(b) DSSS with hard decision decoding (HDD).

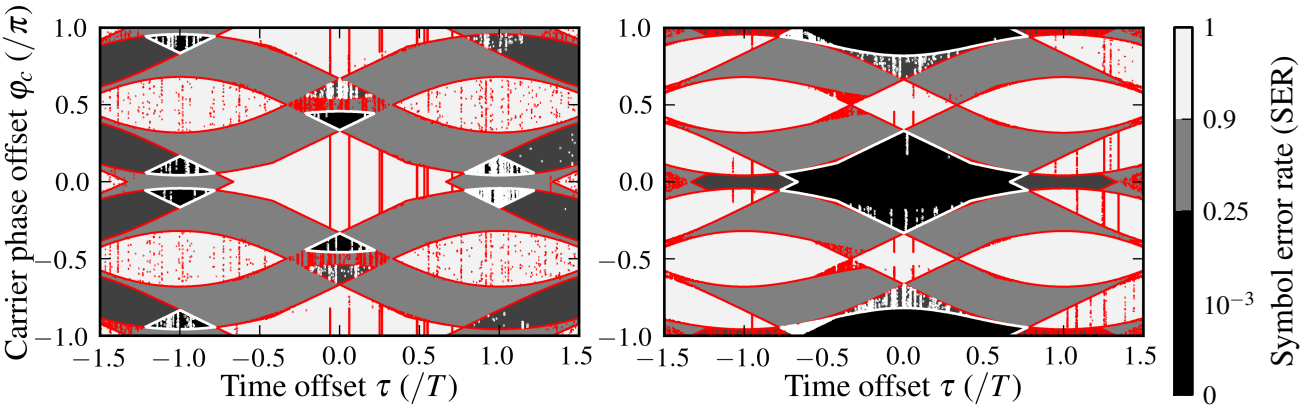


(c) DSSS with soft decision decoding (SDD).

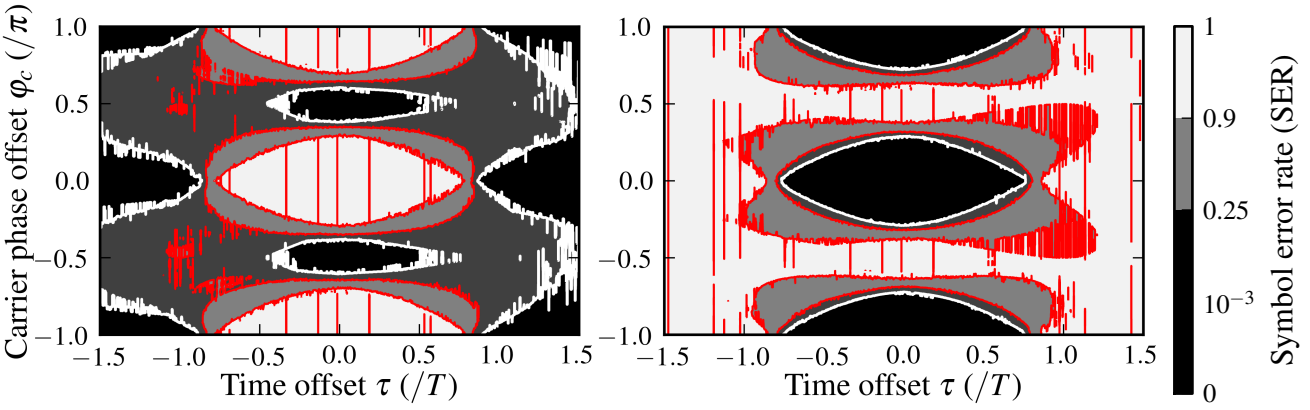
Figure 12. Reception regions of an interfering signal with *independent* payload. For reference the reception threshold for a synchronized signal δ_{SIR} (from Fig. 6a) is also shown.



(a) Uncoded transmissions.



(b) DSSS with hard decision decoding (HDD).



(c) DSSS with soft decision decoding (SDD).

Figure 13. Eye diagrams for the synchronized sender (left) and the interferer (right) for a SIR of -3 dB, illustrating the bit error rate depending on the parameters time offset τ and carrier phase offset φ_c.

1) Reception behavior with small power ratios: In the final evaluation, we analyze the reception behavior of signals with a small difference in power. We consider a the signal power ratio SIR of -3 dB, the results are depicted in Fig. 13.

Uncoded transmissions. In Fig. 13a, we observe that the BER for such transmissions is quite low for both the synchronized sender and the interfering signal. Because the interferer is stronger there is a small central area with small offsets that enables a successful reception.

Hard decision decoding. For HDD, the regions for successful reception are slightly increased in comparison to the uncoded case (Fig. 13b). For the synchronized receiver, there are small reception zones around $\varphi_c = \pm\frac{\pi}{2}$ and $\tau = \pm T$, i.e., the areas where the cos terms are close to zero. For the interferer a second capture zone appears for values of φ_c of $\pm\pi$, which is caused by the use of absolute correlation in the DSSS decoding.

Soft decision decoding. Finally, in the SDD case (Fig. 13c) the reception region for the synchronized sender is increasing for larger time offsets $\tau > T$ and the capture zones are also enlarged. The reception of the interferer already shows capture zones similar to the ones in Fig. 11c, albeit being smaller because of decreased signal power of the interferer.

VI. Experiments

In this section, we provide experimental evidence that our model accurately captures the behavior of existing receiver implementations. Since many results in the previous section comply with existing experimental results, we focus our efforts on the reception of interfering signals because this topic is not well covered experimentally in the literature.

A. Experimental Setup

To perform this experiment, the requirements for the interferer differ from the scope of operation of COTS devices. We need to

- transmit arbitrary symbols on the physical layer, without restrictions like PHY headers,
- synchronize to ongoing transmissions with high accuracy,
- schedule transmissions at a small time granularity.

Because of these requirements, we implemented a custom software radio based system that fulfills them.

1) Interferer implementation: To this end, we modified our USRP2-based experimental system RFReact [29] to recover the timing of the other signal and send arbitrary IEEE 802.15.4 symbols at controlled time offsets. Because of its implementation in the USRP2's FPGA, the system is able to tune the start of transmission with a granularity of 10 ns and send arbitrary waveforms. A detailed description of the system can be found in a technical report [30].

2) Experimental methodology: In our experiments, we consider three parties in the network: a standard-compliant receiver (we monitor the behavior of two implementations to test for hardware dependencies, Atmel AT86RF230 and TI CC2420), a synchronized sender $\mathcal{S}$ (a COTS RZ Raven USB), and the interferer $\mathcal{I}$ described above. The procedure is as follows: $\mathcal{S}$ sends a packet with PHY headers, MAC header, and 8 byte payload. $\mathcal{I}$

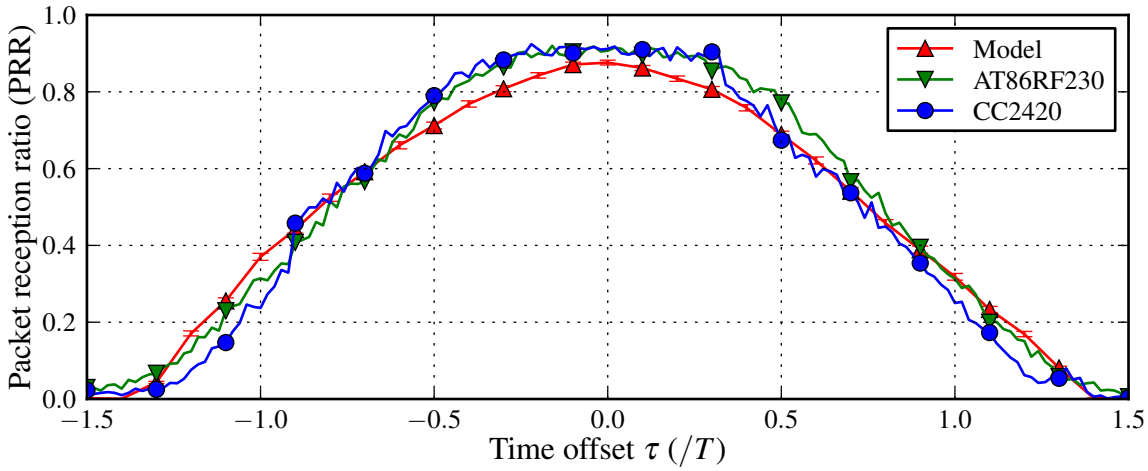


Figure 14. Experimental results for two receiver implementations in comparison to our model. Both receivers display a reception behavior that is well-described by the model.

time-synchronizes with this signal and schedules the transmission of 8 different bytes at the beginning of the payload of $\mathcal{S}$. The receiver first synchronizes on $\mathcal{S}$ and receives its header, but experiences a collision in the payload bits.

We chose values of τ in $(-1.5T; 1.5T)$; for each time offset τ, we send 1,000 packets and analyze the payload detected by the receiver. Based on the results, we derive the PRR as the number of packets with correct payload of the interferer divided by the total number of packets. In other words, we measure the empirical success probability for a message manipulation attack. We derived the value of τ empirically, i.e., we chose the point with maximum PRR in the center as $\tau = 0$. We adjusted the transmit power of $\mathcal{I}$ to result in an SIR of $-40\,\text{dB}$ to be in the region of interest as indicated in Fig. 12c.

B. Experimental Results

The experimental results for the two receiver implementations are shown in Fig. 14. We observe a good fit with our predictions from the model for both receivers, Atmel AT86RF230 and TI CC2420. In the central region, the receivers show a slightly better ability to receive the interfering signal than predicted by our analytical model. The reason is that our model makes the assumptions that no frequency offset is present and that the receiver does not try to resynchronize with a stronger signal. However, receivers must be able to tolerate frequency offsets of up to 100 kHz [1, §6.9.4] and thus track and possibly correct the phase during the packet reception process. Yet, as the results show, our assumptions still yield a good approximation of real receiver behavior. The model provides an excellent fit with the reception behavior of widely used receivers for interfering signals under the assumption of random carrier phase offsets.

VII. Conclusion

In this paper, we presented the first comprehensive analytical model for concurrent transmissions over a wireless channel. As shown in an extensive parameter space

exploration, the model is able to recover insights from experimental results found in the literature and going beyond that, explains the root causes for successful concurrent transmissions exploited in a new generation of network protocols that generate collisions intentionally to increase network throughput or reduce latency. Our results reveal that power capture is not sufficient to explain the performance of these protocols. Rather, coding is an essential factor in the success of these protocols because it crucially widens the capture zone of acceptable signals offsets, increasing the probability of successful reception. Finally, our experimental study of packet reception under collisions shows a good fit and reinforces the validity of our model; as a side product, we demonstrate the feasibility of message manipulation attacks over the air.

REFERENCES

[1] IEEE Standard 802 Part 15.4: Wireless medium access control and physical layer specifications for low-rate WPANs, Sept. 2006.

[2] CARDIERI, P. Modeling interference in wireless ad hoc networks. *IEEE Commun. Surveys Tutorials 12*, 4 (Sept. 2010), 551–572.

[3] CHANG, H., MISRA, V., AND RUBENSTEIN, D. A general model and analysis of physical layer capture in 802.11 networks. In *Proc. of IEEE INFOCOM '06* (Apr. 2006), pp. 1–12.

[4] DAVIS, D., AND GRONEMEYER, S. Performance of slotted ALOHA random access with delay capture and randomized time of arrival. *IEEE Trans. Commun. 28*, 5 (May 1980), 703–710.

[5] DUTTA, P., DAWSON-HAGGERTY, S., CHEN, Y., LIANG, C.-J. M., AND TERZIS, A. Design and evaluation of a versatile and efficient receiver-initiated link layer for low-power wireless. In *Proc. of ACM SenSys '10* (Nov. 2010), ACM, pp. 1–14.

[6] FERRARI, F., ZIMMERLING, M., THIELE, L., AND SAUKH, O. Efficient network flooding and time synchronization with Glossy. In *Proc. of IPSN '11* (Apr. 2011), pp. 73–84.

[7] FOO, J., AND HUANG, D. Multiuser diversity with capture for wireless networks: Protocol and performance analysis. *IEEE J. Sel. Areas Commun. 26*, 8 (Oct. 2008), 1386–1396.

[8] GEZER, C., BURATTI, C., AND VERDONE, R. Capture effect in IEEE 802.15.4 networks: Modelling and experimentation. In *Proc. of IEEE ISWPC '10* (May 2010), pp. 204–209.

[9] GUMMADI, R., WETHERALL, D., GREENSTEIN, B., AND SESHAN, S. Understanding and mitigating the impact of RF interference on 802.11 networks. In *Proc. of ACM SIGCOMM '07* (Sept. 2007), pp. 385–396.

[10] GUPTA, P., AND KUMAR, P. R. The capacity of wireless networks. *IEEE Trans. Inf. T. 46*, 2 (May 2000), 388–404.

[11] IYER, A., ROSENBERG, C., AND KARNIK, A. What is the right model for wireless channel interference? *IEEE Trans. Wireless Commun. 8*, 5 (June 2009), 2662–2671.

[12] JAMIESON, K., AND BALAKRISHNAN, H. PPR: Partial packet recovery for wireless networks. In *Proc. of ACM SIGCOMM '07* (Sept. 2007), pp. 409–420.

[13] KOCHUT, A., VASAN, A., SHANKAR, A., AND AGRAWALA, A. Sniffing out the correct physical layer capture model in 802.11b. In *Proc. of IEEE ICNP '04* (Oct. 2004), pp. 252–261.

[14] LEE, J., KIM, W., LEE, S.-J., JO, D., RYU, J., KWON, T., AND CHOI, Y. An experimental study on the capture effect in 802.11a networks. In *Proc. of ACM WinTECH '07* (Sept. 2007), pp. 19–26.

[15] LEENTVAAR, K., AND FLINT, J. The capture effect in FM receivers. *IEEE Trans. Commun. 24*, 5 (May 1976), 531–539.

[16] LU, J., AND WHITEHOUSE, K. Flash Flooding: Exploiting the capture effect for rapid flooding in wireless sensor networks. In *Proc. of IEEE INFOCOM '09* (Apr. 2009), pp. 2491–2499.

[17] MAHESHWARI, R., JAIN, S., AND DAS, S. R. A measurement study of interference modeling and scheduling in low-power wireless networks. In *Proc. of ACM SenSys '08* (Nov. 2008), pp. 141–154.

[18] MANWEILER, J., SANTHAPURI, N., SEN, S., CHOUDHURY, R. R., NELAKUDITI, S., AND MUNAGALA, K. Order matters: Transmission reordering in wireless networks. *IEEE/ACM Trans. Netw. 20*, 2 (Apr. 2012), 353–366.

[19] POISEL, R. A. *Modern Communications Jamming: Principles and Techniques*. Artech House Publishers, Boston, MA, USA, Nov. 2003.

[20] PÖPPER, C., TIPPENHAUER, N. O., DANEV, B., AND ČAPKUN, S. Investigation of signal and message manipulations on the wireless channel. In *Computer Security — ESORICS 2011* (Sept. 2011), no. 6879 in LNCS, Springer, pp. 40–59.

[21] PROAKIS, J., AND SALEHI, M. *Digital Communications*, 5th ed. McGraw-Hill, New York, NY, USA, Nov. 2007.
[22] RAPPAPORT, T. S. *Wireless Communications: Principles and Practice*, 2nd ed. Prentice-Hall, Upper Saddle River, NJ, USA, Apr. 1996.
[23] SANTHAPURI, N., NELAKUDITI, S., AND CHOUDHURY, R. On spatial reuse and capture in ad hoc networks. In *Proc. of IEEE WCNC '08* (Apr. 2008), pp. 1628–1633.
[24] SHA, M., XING, G., ZHOU, G., LIU, S., AND WANG, X. C-MAC: Model-driven concurrent medium access control for wireless sensor networks. In *Proc. of IEEE INFOCOM '09* (Apr. 2009), pp. 1845–1853.
[25] SON, D., KRISHNAMACHARI, B., AND HEIDEMANN, J. Experimental study of concurrent transmission in wireless sensor networks. In *Proc. of ACM SenSys '06* (Nov. 2006), pp. 237–250.
[26] VUTUKURU, M., JAMIESON, K., AND BALAKRISHNAN, H. Harnessing exposed terminals in wireless networks. In *Proc. of USENIX NSDI '08* (Apr. 2008), pp. 59–72.
[27] WANG, Y., HE, Y., MAO, X., LIU, Y., HUANG, Z., AND LI, X. Exploiting constructive interference for scalable flooding in wireless networks. In *Proc. of IEEE INFOCOM '12* (Mar. 2012), pp. 2104–2112.
[28] WHITEHOUSE, K., WOO, A., JIANG, F., POLASTRE, J., AND CULLER, D. Exploiting the capture effect for collision detection and recovery. In *Proc. of IEEE EmNetS-II* (May 2005), pp. 45–52.
[29] WILHELM, M., MARTINOVIC, I., SCHMITT, J. B., AND LENDERS, V. WiSec '11 demo: RFReact—a real-time capable and channel-aware jamming platform. *SIGMOBILE Mobile Comp. Commun. Rev. 15* (Nov. 2011), 41–42.
[30] WILHELM, M., MARTINOVIC, I., SCHMITT, J. B., AND LENDERS, V. Air dominance in sensor networks: Guarding sensor motes using selective interference. Tech. Rep. arXiv:1305.4038, May 2013.
[31] ZHAO, J., AND GOVINDAN, R. Understanding packet delivery performance in dense wireless sensor networks. In *Proc. of ACM SenSys '03* (Nov. 2003), pp. 1–13.

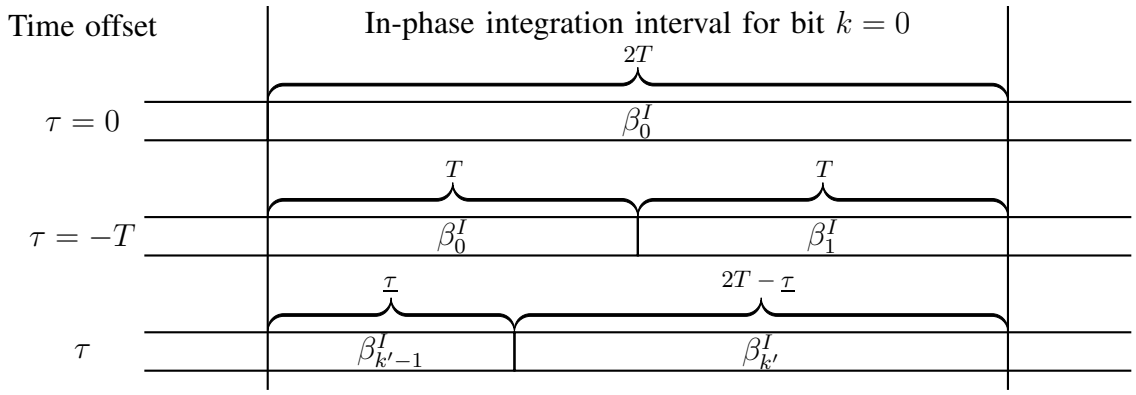


Figure 15. Examples of active bits in the integration interval for the I-bit k. For $\tau = 0$, the only active bit in the integration interval is β_0^I. When the signal starts half a bit-length too early ($\tau = -T$), there are two bits β_0^I and β_1^I that contribute equally to the bit decision, both are active for a duration of T. In the general case of a time offset τ, there are two active bits with indices $\beta_{k'-1}^I$ and $\beta_{k'}^I$, with an active time duration of $\underline{\tau}$ and $2T - \underline{\tau}$, respectively.

APPENDIX A
INTEGRATING RECTANGLE PULSES

A central equation for deriving the influence of individual bits on the demodulator output is the integration of the unit pulse function Π defined in Eq. (4). This is especially important because of signal time offsets τ that shift the pulses relative to the integration interval. Situations that arise are shown in Fig. 15.

To this end, we first derive the general result to the integration over one bit interval k for arbitrary, integrable functions $f(t)$. We consider two variants, the integration of in-phase bits, and the special case of integrating quadrature-phase bits in the bounds of I-bits (which happens when Q-bits leak into the I-phase), i.e.,

$$S_k^I(f) = \int_{(2k-1)T}^{(2k+1)T} b_I(t-\tau) f(t)\, dt$$
$$S_k^Q(f) = \int_{(2k-1)T}^{(2k+1)T} b_Q(t-\tau) f(t)\, dt.$$

Our approach is to split each equation into two parts where the unit pulse is the constant 1 function to simplify the equations. Since only one pulse is active at any point in time, such splitting is possible.

A. Integrating Bit Pulses During the I Integration Interval

1) Integration of I-bits: To perform the integration, we first derive the two indices that have active pulses during the integration interval. The shift introduced by τ lead to the two new bits with indices $k' = k - \left\lfloor \frac{\tau}{2T} \right\rfloor$ and $k' - 1$. The remaining time offset inside the selected bits is $\underline{\tau} = \tau - 2k_\tau T$, i.e., each of the two bits is active for the time interval $\underline{\tau}$ and $2T - \underline{\tau}$, respectively. Because of this definition, the values of $\underline{\tau}$ are restricted to the interval $(0, 2T)$—negative values would activate previous bits, which is prevented by the floor operation.

For the in-phase component, we derive

$$
\begin{aligned}
&S_k^I(f) \\
&= \int_{(2k-1)T}^{(2k+1)T} b_I(t-\tau) f(t)\, dt \\
&= \int_{(2k-1)T}^{(2k+1)T} b_I(t-2k_\tau T-\underline{\tau}) f(t)\, dt \\
&= \int_{(2k-1)T}^{(2k+1)T} \sum_{k=-\infty}^{\infty} \beta_k^I \Pi\left(\frac{t-\underline{\tau}-(k+k_\tau)2T}{2T}\right) f(t)\, dt
\end{aligned}
$$

Re-labeling the bit indices k to k' (note: positive time shifts lead to negative index shifts)

$$
\begin{aligned}
&= \int_{(2k-1)T}^{(2k+1)T} \left(\beta_{k'-1}^I \Pi\left(\frac{t-\underline{\tau}-(k-1)2T}{2T}\right) + \beta_{k'}^I \Pi\left(\frac{t-\underline{\tau}-2kT}{2T}\right)\right) f(t)\, dt \\
&= \beta_{k'-1}^I \int_{(2k-1)T}^{(2k+1)T} \Pi\left(\frac{t-\underline{\tau}-(k-1)2T}{2T}\right) f(t)\, dt + \beta_{k'}^I \int_{(2k-1)T}^{(2k+1)T} \Pi\left(\frac{t-\underline{\tau}-2kT}{2T}\right) f(t)\, dt
\end{aligned}
$$

Use the fact that the shifted pulses are zero during parts of the integration interval

$$
= \beta_{k'-1}^I \int_{(2k-1)T}^{(2k-1)T+\underline{\tau}} \Pi\left(\frac{t-\underline{\tau}-(k-1)2T}{2T}\right) f(t)\, dt + \beta_{k'}^I \int_{(2k-1)T+\underline{\tau}}^{(2k+1)T} \Pi\left(\frac{t-\underline{\tau}-2kT}{2T}\right) f(t)\, dt
$$

The Π pulses are constant 1 in the new integration intervals

$$
\begin{aligned}
&= \beta_{k'-1}^I \int_{(2k-1)T}^{(2k-1)T+\underline{\tau}} f(t)\, dt + \beta_{k'}^I \int_{(2k-1)T+\underline{\tau}}^{(2k+1)T} f(t)\, dt \\
&= \beta_{k'-1}^I \left[F(t)\right]_{2kT-T}^{2kT-T+\underline{\tau}} + \beta_{k'}^I \left[F(t)\right]_{2kT-T+\underline{\tau}}^{2kT+T}
\end{aligned}
$$

If the function to integrate is the constant 1 function ($f(t)=1$), then we derive

$$
S_k^I(1) = \underline{\tau}\beta_{k'-1}^I + (2T-\underline{\tau})\beta_{k'}^I \tag{15}
$$

2) Integration of Q-bits: When Q bits leak into the in-phase, we have the consider the additional shift of T due to the staggering of bits in the MSK modulation. We provide the derivation of this special case here. First, we substitute the timing offset τ with $\tau^Q = \tau + T$ to accommodate of the staggering. Second, the bit indices must be re-adjusted because of the shift; the new index is denoted by $k^{Q\prime} = k - \lfloor (\tau + T)/2T \rfloor$. For the case of the constant 1 function, we derive then

$$S_k^Q(1) = \underline{\tau^Q}\beta_{k^{Q\prime}-1}^Q + \left(2T - \underline{\tau^Q}\right)\beta_{k^{Q\prime}}^Q. \tag{16}$$

B. Deriving Special Cases: $S_k^I(\cos 2\omega_p t)$ and $S_k^Q(\cos 2\omega_p t)$

1) Integration of I-bits: We derive the result of bit pulse integration for this special case.

$$\begin{aligned}
&S_k^I(\cos 2\omega_p t) \\
&= \int_{(2k-1)T}^{(2k+1)T} b_I(t-\tau)\cos 2\omega_p t\, dt \\
&= \beta_{k'-1}^I \left[\frac{1}{2\omega_p}\sin 2\omega_p t\right]_{(2k-1)T}^{(2k-1)T+\underline{\tau}} + \beta_{k'}^I \left[\frac{1}{2\omega_p}\sin 2\omega_p t\right]_{(2k-1)T+\underline{\tau}}^{(2k+1)T} \\
&= \frac{\beta_{k'-1}^I}{2\omega_p}\left[\sin 2\omega_p t\right]_{(2k-1)T}^{(2k-1)T+\underline{\tau}} + \frac{\beta_{k'}^I}{2\omega_p}\left[\sin 2\omega_p t\right]_{(2k-1)T+\underline{\tau}}^{(2k+1)T}
\end{aligned}$$

Performing the integration results in (we denote $\omega_p\underline{\tau} = \underline{\varphi_p}$):

$$\begin{aligned}
&= \frac{\beta_{k'-1}^I}{2\omega_p}\left[\sin\left((2k-1)\pi + 2\underline{\varphi_p}\right) - \sin\left((2k-1)\pi\right)\right] \\
&\quad + \frac{\beta_{k'}^I}{2\omega_p}\left[\sin\left((2k+1)\pi\right) - \sin\left((2k-1)\pi + 2\underline{\varphi_p}\right)\right] \\
&= \frac{\beta_{k'-1}^I}{2\omega_p}\left[\sin\left(-\pi + 2\underline{\varphi_p}\right) - \sin(-\pi)\right] + \frac{\beta_{k'}^I}{2\omega_p}\left(\sin\pi + \sin 2\underline{\varphi_p}\right) \\
&= -\frac{\beta_{k'-1}^I}{2\omega_p}\sin 2\underline{\varphi_p} + \frac{\beta_{k'}^I}{2\omega_p}\sin 2\underline{\varphi_p} \\
&= \sin 2\underline{\varphi_p}\left(-\frac{\beta_{k'-1}^I}{2\omega_p} + \frac{\beta_{k'}^I}{2\omega_p}\right)
\end{aligned}$$

Using $\sin 2\underline{\varphi_p} = \sin\left(2\omega_p(\tau - 2k_\tau T)\right) = \sin\left(2\varphi_p - 2k_\tau\pi\right) = \sin 2\varphi_p$

$$= -\frac{1}{2\omega_p}\sin 2\varphi_p\left(\beta_{k'-1}^I - \beta_{k'}^I\right)$$

The overall result is

$$S_k^I(\cos 2\omega_p t) = -\frac{1}{2\omega_p}\sin 2\varphi_p\left(\beta_{k'-1}^I - \beta_{k'}^I\right) \tag{17}$$

2) Integration of Q-bits: In this case, the use of τ^Q leads to a different phase shift $\varphi_p^Q = \omega_p(\tau + T) = \omega_p\tau + \frac{\pi T}{2T} = \varphi_p + \frac{\pi}{2}$ that leads to changes in the integration. Using the following two simplifications the derivation can be performed analogously to the previous subsection.

$$\sin 2\underline{\varphi_p^Q} = \sin 2\omega_p\underline{\tau^Q} = \sin\left(2\frac{\pi}{2T}\left(\tau^Q - 2k_\tau^Q T\right)\right) = \sin\left(\frac{\tau^Q\pi}{T} - 2k_\tau^Q\pi\right) = \sin 2\varphi_p^Q$$

and

$$\sin 2\varphi_p^Q = \sin(2\varphi_p + \pi) = -\sin 2\varphi_p$$

The overall result is

$$S_k^Q(\cos 2\omega_p t) = \frac{1}{2\omega_p}\sin 2\varphi_p\left(\beta_{k^{Q\prime}-1}^Q - \beta_{k^{Q\prime}}^Q\right) \tag{18}$$

C. Deriving Special Cases: $S_k^I(\sin 2\omega_p t)$ and $S_k^Q(\sin 2\omega_p t)$

1) Integration of I-bits: We derive the result of bit pulse integration for this special case.

$$\begin{aligned}
&S_k^I(\sin 2\omega_p t)\\
&= \int_{(2k-1)T}^{(2k+1)T} b_I(t-\tau)\sin 2\omega_p t\, dt\\
&= \beta_{k'-1}^I\left[-\frac{1}{2\omega_p}\cos 2\omega_p t\right]_{(2k-1)T}^{(2k-1)T+\underline{\tau}} + \beta_{k'}^I\left[-\frac{1}{2\omega_p}\cos 2\omega_p t\right]_{(2k-1)T+\underline{\tau}}^{(2k+1)T}\\
&= -\frac{\beta_{k'-1}^I}{2\omega_p}\left[\cos 2\omega_p t\right]_{(2k-1)T}^{(2k-1)T+\underline{\tau}} - \frac{\beta_{k'}^I}{2\omega_p}\left[\cos 2\omega_p t\right]_{(2k-1)T+\underline{\tau}}^{(2k+1)T}
\end{aligned}$$

Performing the integration results in (we denote $\omega_p\underline{\tau} = \underline{\varphi_p}$):

$$\begin{aligned}
&= -\frac{\beta_{k'-1}^I}{2\omega_p}\left[\cos\left((2k-1)\pi + 2\underline{\varphi_p}\right) - \cos\left((2k-1)\pi\right)\right]\\
&\quad - \frac{\beta_{k'}^I}{2\omega_p}\left[\cos\left((2k+1)\pi\right) - \cos\left((2k-1)\pi + 2\underline{\varphi_p}\right)\right]\\
&= -\frac{\beta_{k'-1}^I}{2\omega_p}\left(\cos\left(-\pi + 2\underline{\varphi_p}\right) - \cos(-\pi)\right) - \frac{\beta_{k'}^I}{2\omega_p}\left(\cos\pi - \cos\left(-\pi + 2\underline{\varphi_p}\right)\right)\\
&= -\frac{\beta_{k'-1}^I}{2\omega_p}\left(1 - \cos 2\underline{\varphi_p}\right) + \frac{\beta_{k'}^I}{2\omega_p}\left(1 - \cos 2\underline{\varphi_p}\right)\\
&= -\frac{1}{2\omega_p}\left(1 - \cos 2\underline{\varphi_p}\right)\left(\beta_{k'-1}^I - \beta_{k'}^I\right)
\end{aligned}$$

Using $\cos 2\underline{\varphi_p} = \cos\left(2\omega_p\left(\tau - 2k_\tau T\right)\right) = \cos\left(2\varphi_p - 2k_\tau\pi\right) = \cos 2\varphi_p$

$$= -\frac{1}{2\omega_p}\left(1 - \cos 2\varphi_p\right)\left(\beta^I_{k'-1} - \beta^I_{k'}\right)$$

The overall result is

$$S^I_k\left(\sin 2\omega_p t\right) = -\frac{1}{2\omega_p}\left(1 - \cos 2\varphi_p\right)\left(\beta^I_{k'-1} - \beta^I_{k'}\right) \tag{19}$$

2) Integration of Q-bits: This case can be performed analogously to Section A-B, with the following two simplifications:

$$\cos 2\underline{\varphi^Q_p} = \cos 2\omega_p\underline{\tau^Q} = \cos\left(2\frac{\pi}{2T}\left(\tau^Q - 2k^Q_\tau T\right)\right) = \cos\left(\frac{\tau^Q\pi}{T} - 2k^Q_\tau\pi\right) = \cos 2\varphi^Q_p$$

and

$$\cos 2\varphi^Q_p = \cos\left(2\varphi_p + \pi\right) = -\cos 2\varphi_p$$

The overall result is

$$S^Q_k\left(\sin 2\omega_p\left(t\right)\right) = \frac{1}{2\omega_p}\left(1 + \cos 2\varphi_p\right)\left(\beta^Q_{k^{Q\prime}-1} - \beta^Q_{k^{Q\prime}}\right) \tag{20}$$

APPENDIX B
DEMODULATOR OUTPUT FOR SIGNALS WITH BOTH OFFSETS τ, φ_c

With the tools presented in Appendix A, we can now proceed to prove Theorem 1.

Theorem 1. *For an interfering MSK signal $u(t)$ with parameters τ and φ_c, the contribution to the demodulation output $\Lambda_u^I(k)$ is given by*

$$\Lambda_u^I(k) = \frac{1}{4}A_u \left\{ \cos\varphi_c \left[\cos\varphi_p \left(\underline{\tau}\beta_{k'-1}^I + (2T - \underline{\tau})\beta_{k'}^I \right) - \frac{2T}{\pi} \sin\varphi_p \left(\beta_{k'-1}^I - \beta_{k'}^I \right) \right] \right.$$
$$\left. - \sin\varphi_c \left[\sin\varphi_p \left(\underline{\tau^Q}\beta_{k^{Q'}-1}^Q + \left(2T - \underline{\tau^Q}\right)\beta_{k^{Q'}}^Q \right) + \frac{2T}{\pi} \cos\varphi_p \left(\beta_{k^{Q'}-1}^Q - \beta_{k^{Q'}}^Q \right) \right] \right\}.$$

Proof: We first derive the resulting signal after demodulation.

$$\begin{aligned}
&u(t)\,\phi_I(t) \\
&= A_u \left[b_I(t-\tau)\cos(\omega_p t - \varphi_p)\cos(\omega_c t + \varphi_c) \right. \\
&\qquad \left. + b_Q(t-\tau)\sin(\omega_p t - \varphi_p)\sin(\omega_c t + \varphi_c) \right] [\cos\omega_p t \cos\omega_c t] \\
&= A_u \left[(b_I(t-\tau)\cos(\omega_p t - \varphi_p)\cos\omega_p t \cos(\omega_c t + \varphi_c)\cos\omega_c t) \right. \\
&\qquad \left. + (b_Q(t-\tau)\sin(\omega_p t - \varphi_p)\cos\omega_p t \sin(\omega_c t + \varphi_c)\cos\omega_c t) \right] \\
&= \frac{A_u}{4} \left[(b_I(t-\tau)(\cos\varphi_p + \cos(2\omega_p t - \varphi_p))(\cos\varphi_c + \cos(2\omega_c t + \varphi_c))) \right. \\
&\qquad \left. + (b_Q(t-\tau)(\sin(-\varphi_p) + \sin(2\omega_p t - \varphi_p))(\sin\varphi_c + \sin(2\omega_c t + \varphi_c))) \right]
\end{aligned}$$

We apply perfect lowpass filtering ($\star$) to filter out high-frequency components ($2\omega_c t$)

$$\begin{aligned}
&\stackrel{\star}{=} \frac{A_u}{4} \left[(b_I(t-\tau)\cos\varphi_c(\cos\varphi_p + \cos(2\omega_p t - \varphi_p))) \right. \\
&\qquad \left. + (b_Q(t-\tau)\sin\varphi_c(\sin(2\omega_p t - \varphi_p) - \sin\varphi_p)) \right] \\
&= \frac{A_u}{4} \left[(b_I(t-\tau)\cos\varphi_c(\cos\varphi_p + \cos 2\omega_p t\cos\varphi_p + \sin 2\varphi_p t \sin\varphi_p)) \right. \\
&\qquad \left. + (b_Q(t-\tau)\sin\varphi_c(-\sin\varphi_p + \sin 2\omega_p t\cos\varphi_p - \cos 2\omega_p t \sin\varphi_p)) \right]
\end{aligned}$$

The bit decision is performed by integration over the bit interval k.

$$\begin{aligned}
&\int_{(2k-1)T}^{(2k+1)T} u(t)\,\phi_I(t)\,dt \\
&= \frac{A_u}{4} \left[\cos\varphi_c \int_{(2k-1)T}^{(2k+1)T} b_I(t-\tau)(\cos\varphi_p + \cos 2\omega_p t\cos\varphi_p + \sin 2\varphi_p t\sin\varphi_p)\,dt \right. \\
&\qquad \left. + \sin\varphi_c \int_{(2k-1)T}^{(2k+1)T} b_Q(t-\tau)(-\sin\varphi_p + \sin 2\omega_p t\cos\varphi_p - \cos 2\omega_p t\sin\varphi_p)\,dt \right] \\
&= \frac{A_u}{4} \left[\cos\varphi_c \mathcal{X}_1 + \sin\varphi_c \mathcal{X}_2 \right]
\end{aligned}$$

We derive the results for both terms $\mathcal{X}_1$ and $\mathcal{X}_2$ individually in the following two sections.

Putting the two results in Eq. (21) and Eq. (22) together, the overall result is

$$\begin{aligned}
&\int_{(2k-1)T}^{(2k+1)T} u(t)\,\phi_I(t)\,dt \\
&= \frac{A_u}{4}\left\{\cos\varphi_c\left[\cos\varphi_p\left(\underline{\tau}\beta^I_{k'-1} + (2T-\underline{\tau})\,\beta^I_{k'}\right) - \frac{2T}{\pi}\sin\varphi_p\left(\beta^I_{k'-1} - \beta^I_{k'}\right)\right]\right. \\
&\qquad \left. - \sin\varphi_c\left[\sin\varphi_p\left(\underline{\tau^Q}\beta^Q_{kQ'-1} + \left(2T-\underline{\tau^Q}\right)\beta^Q_{kQ'}\right) + \frac{2T}{\pi}\cos\varphi_p\left(\beta^Q_{kQ'-1} - \beta^Q_{kQ'}\right)\right]\right\}
\end{aligned}$$

■

A. Integrating the Term $\mathcal{X}_1$

$$\begin{aligned}
&\int_{(2k-1)T}^{(2k+1)T} b_I(t-\tau)\left(\cos\varphi_p + \cos 2\omega_p t\cos\varphi_p + \sin 2\varphi_p t\sin\varphi_p\right)dt \\
&= \cos\varphi_p\int_{(2k-1)T}^{(2k+1)T} b_I(t-\tau)\,dt + \cos\varphi_p\int_{(2k-1)T}^{(2k+1)T} b_I(t-\tau)\cos 2\omega_p t\,dt \\
&\quad + \sin\varphi_p\int_{(2k-1)T}^{(2k+1)T} b_I(t-\tau)\sin 2\omega_p t\,dt \\
&= \cos\varphi_p S^I_k(1) + \cos\varphi_p S^I_k(\cos 2\omega_p t) + \sin\varphi_p S^I_k(\sin 2\omega_p t)
\end{aligned}$$

By using the results in Appendix A (Eqs. (15), (17) and (19)), we can reformulate this equation to

$$\begin{aligned}
&= \cos\varphi_p\left(\underline{\tau}\beta^I_{k'-1} + (2T-\underline{\tau})\,\beta^I_{k'}\right) \\
&\quad - \frac{\beta^I_{k'-1}}{2\omega_p}\left(\cos\varphi_p\sin 2\varphi_p + \sin\varphi_p\left(1-\cos 2\varphi_p\right)\right) + \frac{\beta^I_{k'}}{2\omega_p}\left(\cos\varphi_p\sin 2\varphi_p + \sin\varphi_p\left(1-\cos 2\varphi_p\right)\right)
\end{aligned}$$

Simplifying this equation yields the desired result.

$$\begin{aligned}
&= \cos\varphi_p\left(\underline{\tau}\beta^I_{k'-1} + (2T-\underline{\tau})\,\beta^I_{k'}\right) - \left(\frac{\beta^I_{k'-1}-\beta^I_{k'}}{2\omega_p}\right)\left(\sin 2\varphi_p\cos\varphi_p - \cos 2\varphi_p\sin\varphi_p + \sin\varphi_p\right) \\
&= \cos\varphi_p\left(\underline{\tau}\beta^I_{k'-1} + (2T-\underline{\tau})\,\beta^I_{k'}\right) - \frac{\sin\varphi_p}{\omega_p}\left(\beta^I_{k'-1} - \beta^I_{k'}\right) \\
&= \cos\varphi_p\left(\underline{\tau}\beta^I_{k'-1} + (2T-\underline{\tau})\,\beta^I_{k'}\right) - \frac{2T}{\pi}\sin\varphi_p\left(\beta^I_{k'-1} - \beta^I_{k'}\right)
\end{aligned}$$

In the second step in the previous equation, we used the following simplification:

$$\begin{aligned}
&\sin 2\varphi_p\cos\varphi_p - \cos 2\varphi_p\sin\varphi_p + \sin\varphi_p \\
&= 2\cos^2\varphi_p\sin\varphi_p - \left(2\cos^2\varphi_p - 1\right)\sin\varphi_p + \sin\varphi_p \\
&= \left(2\cos^2\varphi_p - 2\cos^2\varphi_p + 1 + 1\right)\sin\varphi_p \\
&= 2\sin\varphi_p
\end{aligned}$$

Overall, the result is

$$\mathcal{X}_1 = \cos\varphi_p \left(\underline{\tau}\beta^I_{k'-1} + (2T - \underline{\tau})\,\beta^I_{k'}\right) - \frac{2T}{\pi}\sin\varphi_p \left(\beta^I_{k'-1} - \beta^I_{k'}\right) \tag{21}$$

B. Integrating the Term $\mathcal{X}_2$

We will now derive the second integral. We must use the rules for Q pulse integration with I intervals.

$$\begin{aligned}
&\int_{(2k-1)T}^{(2k+1)T} b_Q\left(t-\tau\right)\left(-\sin\varphi_p - \cos 2\omega_p t \sin\varphi_p + \sin 2\omega_p t\cos\varphi_p\right) dt \\
&= -\left[\int_{(2k-1)T}^{(2k+1)T} b_Q\left(t-\tau\right)\sin\varphi_p dt + \int_{(2k-1)T}^{(2k+1)T} b_Q\left(t-\tau\right)\cos 2\omega_p t\sin\varphi_p dt\right. \\
&\quad \left. - \int_{(2k-1)T}^{(2k+1)T} b_Q\left(t-\tau\right)\sin 2\omega_p t\cos\varphi_p dt\right] \\
&= -\left[\sin\varphi_p S^Q_k\left(1\right) + \sin\varphi_p S^Q_k\left(\cos 2\omega_p t\right) - \cos\varphi_p S^Q_k\left(\sin 2\omega_p t\right)\right]
\end{aligned}$$

By using the results in Appendix A (Eqs. (16), (18) and (20)), we can reformulate this equation to

$$\begin{aligned}
&= -\sin\varphi_p\left(\underline{\tau^Q}\beta^Q_{kQ'-1} + \left(2T - \underline{\tau^Q}\right)\beta^Q_{kQ'}\right) \\
&\quad - \frac{1}{2\omega_p}\left(\sin\varphi_p\sin 2\varphi_p - \cos\varphi_p\left(1+\cos 2\varphi_p\right)\right)\left(\beta^Q_{kQ'-1} - \beta^Q_{kQ'}\right)
\end{aligned}$$

Simplifying yield the desired result

$$\begin{aligned}
&= -\sin\varphi_p\left(\underline{\tau^Q}\beta^Q_{kQ'-1} + \left(2T - \underline{\tau^Q}\right)\beta^Q_{kQ'}\right) \\
&\quad - \frac{1}{2\omega_p}\left(\sin 2\varphi_p\sin\varphi_p + \cos 2\varphi_p\cos\varphi_p + \cos\varphi_p\right)\left(\beta^Q_{kQ'-1} - \beta^Q_{kQ'}\right) \\
&= -\left[\sin\varphi_p\left(\underline{\tau^Q}\beta^Q_{kQ'-1} + \left(2T - \underline{\tau^Q}\right)\beta^Q_{kQ'}\right) + \frac{2T}{\pi}\cos\varphi_p\left(\beta^Q_{kQ'-1} - \beta^Q_{kQ'}\right)\right]
\end{aligned}$$

In the last step, we used the following simplification

$$\begin{aligned}
&\sin 2\varphi_p\sin\varphi_p + \cos\varphi_p + \cos 2\varphi_p\cos\varphi_p \\
&= 2\sin^2\varphi_p\cos\varphi_p + \cos\varphi_p + \left(1 - 2\sin^2\varphi_p\right)\cos\varphi_p \\
&= \left(2\sin^2\varphi_p + 1 + 1 - 2\sin^2\varphi_p\right)\cos\varphi_p \\
&= 2\cos\varphi_p
\end{aligned}$$

Overall, the result is

$$\mathcal{X}_2 = -\left[\sin\varphi_p\left(\underline{\tau^Q}\beta^Q_{kQ'-1} + \left(2T - \underline{\tau^Q}\right)\beta^Q_{kQ'}\right) + \frac{2T}{\pi}\cos\varphi_p\left(\beta^Q_{kQ'-1} - \beta^Q_{kQ'}\right)\right] \tag{22}$$