

Differentiating Clear Channel Assessment using Transmit Power Variation

ALEX KING, School of Computing and Communications, Lancaster University, UK

UTZ ROEDIG, School of Computing and Communications, Lancaster University, UK

Clear Channel Assessment (CCA) is a core element of Wireless Sensor Network (WSN) Medium Access Control (MAC) protocols which is used on transmitter and receiver side. Current CCA implementations cannot determine the device type occupying the media, leaving nodes unable to differentiate between WSN traffic and interference. However, this would be valuable as MAC protocols benefit from reacting differently depending on the channel occupier. In this paper we describe a method called Power Differentiating Clear Channel Assessment (P-DCCA). Transmitters vary the output power of the radio while the packet is being sent. Receivers are able to identify signals with this characteristic, enabling a Differentiating Clear Channel Assessment (DCCA) check to reveal if the medium is currently occupied by WSN traffic or other interference. We present an implementation and thorough evaluation of P-DCCA. Using ContikiMAC as example we describe how P-DCCA can be integrated within MAC protocols. We show via large-scale testbed experiments and deployments that P-DCCA enabled networks have a significant improved performance. For example, we show that a P-DCCA enabled network can improve Packet Reception Rate (PRR) by up to a factor of 10 while reducing energy usage by over 80% under heavy interference.

CCS Concepts: • **Computer systems organization** → **Sensor networks**;

Additional Key Words and Phrases: Medium Access Control, Radio Interference, Network Coexistence

ACM Reference Format:

Alex King and Utz Roedig. 2018. Differentiating Clear Channel Assessment using Transmit Power Variation. *ACM Trans. Sensor Netw.* 1, 1, Article 1 (January 2018), 28 pages. <https://doi.org/0000001.0000001>

1 INTRODUCTION

Wireless Sensor Networks (WSNs) are often deployed in environments where they have to coexist with other networks. For example, it is common to find 802.15.4 based WSNs sharing the transmission medium with 802.11 type WiFi. The state of the communication medium (busy or idle) is used to determine WSN node behaviour. Before transmitting, nodes use this information to decide if a packet can be transmitted or if the communication attempt should be deferred (back-off). On the receiving side nodes use this information to determine if the radio should remain in a power efficient sleep state, or be awoken to receive an incoming packet. Transceiver chips implement a Clear Channel Assessment (CCA) which allows nodes to sample briefly the channel and to determine its state. The available CCA method of currently used 802.15.4 transceiver chips only indicates if the channel is busy or idle; it is not possible to determine the network type currently occupying the channel.

However, in many situations such information would be beneficial as node behaviour could then be tuned more aptly, to improve network performance and energy efficiency. Transmitters may employ different back-off strategies depending on the node type currently occupying the channel. For example, knowing that a comparatively short WiFi transmission is occupying the channel, a

Authors' addresses: Alex King, School of Computing and Communications, Lancaster University, Lancaster University, Lancaster, LA1 4WA, UK; Utz Roedig, School of Computing and Communications, Lancaster University, Lancaster University, Lancaster, LA1 4WA, UK, u.roedig@lancaster.ac.uk.

© 2018 Copyright held by the owner/author(s). Publication rights licensed to the Association for Computing Machinery. This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in *ACM Transactions on Sensor Networks*, <https://doi.org/0000001.0000001>.

sensor node may back-off for a much shorter duration than it would when detecting an 802.15.4 transmission. Receivers may decide on different sleep patterns depending on the current channel occupation, such as not extending the node wake cycle if the occupying transmitter is not part of the 802.15.4 WSN.

Implementing CCA capable of interference differentiation on current WSN hardware is extremely challenging due to the limitations of the low power radio, such as the commonly used TI CC2420 and its newer derivatives. Previous works on interference classification have proven that high accuracy is achievable on limited resources. However, these existing works operate on timescales far exceeding the standard CCA duration, precluding a like-for-like replacement.

In this paper we overcome this limitation and describe a novel method for Differentiating Clear Channel Assessment (DCCA) compatible with current off-the-shelf transceiver hardware such as the TI CC2420. Transmitters in an 802.15.4 WSN network vary the transmission power during packet transmission. Receivers can then identify this encoded information during a brief CCA check, allowing nodes to determine if the channel is currently occupied by a node belonging to the same WSN network or not. We refer to this CCA implementation as Power Differentiating Clear Channel Assessment (P-DCCA). The focus of our work presented in this paper is on the core P-DCCA mechanism. We do not aim to detail in this work optimal policies for particular MAC protocols using P-DCCA. However, we show using ContikiMAC [9] that even the implementation of very simple policies based on P-DCCA lead to tremendous performance improvements.

This paper provides the following contributions:

- *P-DCCA – DCCA based on transmit power variation*: A novel method for Differentiating Clear Channel Assessment (DCCA) based on variations in transmission power output is described. A P-DCCA check reveals if the transmission medium is occupied by another WSN node or if external interference is occupying the channel.
- *P-DCCA evaluation*: A detailed evaluation of P-DCCA is given. Specifically, we evaluate detection accuracy, cost in terms of energy consumption and the impact on transmission range. We show that a channel occupier can be identified correctly in 88% of cases for 802.15.4, 94% of cases for other interference, and that P-DCCA requires little more energy than a normal CCA check. We also quantify the impact of power variation on achievable communication range (30% range reduction in a typical setting). We compare P-DCCA with the closest related mechanism ZiSense – although it cannot be considered as like-for-like replacement – and show that it outperforms this existing alternative.
- *P-DCCA application*: We showcase P-DCCA as part of ContikiMAC, and evaluate in settings where the network must coexist with WiFi devices. Our evaluation, which includes a 49-node testbed experiment, shows that P-DCCA significantly improves packet reception (up to ten-fold increase) and energy usage (over 80% reduction), under heavy interference.

The remaining paper is organised as follows. In the next section we discuss CCA, how CCA is used in power efficient MAC protocols and general DCCA options. Section 3 describes P-DCCA, the DCCA method based on transmit power variation. In this section we also give a brief overview of ZiSense, an alternative mechanism we used for comparison in our evaluation. The accuracy and energy efficiency of P-DCCA is evaluated in Sections 4 and 5 respectively. Following this, the communication range of P-DCCA is evaluated in Section 6. In Section 7 we describe, as an application example, how P-DCCA can improve performance of WSN nodes using ContikiMAC. We show WSN network performance improvements in interference environments when using P-DCCA. Practical deployments and large-scale testbed experiments are used to showcase the usefulness of P-DCCA. Section 8 presents related work and Section 9 concludes the paper.

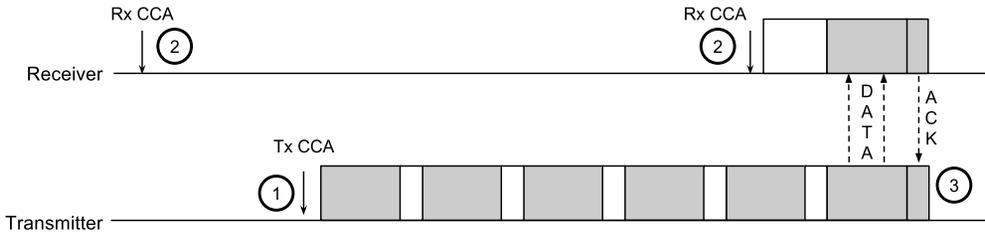


Fig. 1. Operation of LPL MAC protocols: 1) Transmit request followed by CCA check, then packet strobos. 2) Periodic receiver CCA check to listen for incoming packets. 3) After data is received, an ACK is transmitted, packet strobos stop.

2 PRELIMINARY DISCUSSION

The 802.15.4 physical layer is a common choice for WSNs due to its low power consumption and suitability for low data rate applications. The 2.4 GHz frequency is shared with other protocols and devices; as their prevalence continues to increase, parallel deployments with 802.15.4 are becoming more common. Without due consideration to network coexistence, network performance is sub-optimal. Sources of interference include Bluetooth, WiFi, and other 802.15.4 devices, as well as non-communication devices such as microwave ovens.

2.1 CCA and the Case for DCCA

WSN MAC protocols use CCA on the transmitter and receiver side. As CCA only allows us to distinguish a busy from an idle channel the same policy must be used for all channel busy cases. However, a less ambiguous CCA response would be advantageous, allowing nodes to implement a response dependent on the nature of the interference.

Transmitter CCA. 802.15.4 nodes must assess the state of the channel before transmitting data to avoid collisions with other nodes and to increase the likelihood of the data being received (see Figure 1). For example, a sender will defer and retry later upon detecting other channel activity - presumed likely to corrupt any transmission attempt. CCA checks are commonly used for this purpose: briefly sampling the channel and indicating the current state. Currently used CCA implementations offer an energy threshold indicator: busy if the energy on the channel exceeds a set threshold, free otherwise. As noise can lead to a false channel assessment, CCA methods have been devised which analyse a number of consecutive CCA checks together [21]. Such outlier detection improves channel assessment but it can still only be decided if the channel is free or not. This ambiguity requires MAC protocols to implement a single policy in response to all interference.

However, to improve network performance senders can opt to ignore interference from sources outside the network, as the recipient may still be able to receive the packet over the interference. This response is reasonable in cases without mutual channel etiquette, such as WiFi. Alternatively, the transmitter can apply different back-off timing depending on the interference source. When competing with WiFi nodes for a channel, much shorter back-off timers are required than in a case where competing with other 802.15.4 nodes. The optimal response policy depends on the MAC protocol used, the coexisting network(s) and the traffic patterns in the network.

Receiver CCA. CCA is also used on the receiving side of energy efficient WSN MAC protocols, such as ContikiMAC [9] (see Figure 1). The radio is the greatest source of power consumption in most sensor nodes, often dictating network lifetime. Thus, MAC protocols seek to leave the radio

in an energy efficient sleep state, retaining operational information (such as channel, transmission power), but unable to send or receive packets. In order to receive data, nodes must periodically listen to the channel for incoming transmissions, a period defined by the *duty cycle*. A node wishing to send data to another node must transmit repeatedly to the recipient throughout this duty cycle, terminating only if an acknowledgement has been received, or a timeout has occurred.

Due to the small energy cost and immediate response, CCA is commonly used to sample the channel, quickly indicating the channel state. Detecting an occupied channel, the radio is left powered on to receive any subsequent packet, otherwise returning the radio to a sleep state.

Once again, the ambiguity of CCA requires nodes to implement a single policy in response to any channel activity. In environments frequented by other interference, this leads to increased *false wake-ups*, where nodes listen to the channel in response to spurious interference, wasting energy. To improve energy consumption a node can implement different policies in regard to the interference type detected. It is sensible to prevent a wake-up in case of non-802.15.4 traffic.

2.2 DCCA Options

As shown, DCCA is a valuable building block for MAC protocols and the question is how it can be realised. We consider three possible avenues to realise DCCA: Modulation Detection Differentiating Clear Channel Assessment (MD-DCCA), Time Differentiating Clear Channel Assessment (T-DCCA), and P-DCCA.

Modulation Detection Differentiating Clear Channel Assessment (MD-DCCA). The 802.15.4 standard defines modulation detection as an optional CCA method - indicating busy if a signal with the correct modulation and spreading characteristics is detected. Alongside energy detection, this would be ideal for implementing DCCA with little processing overhead. This approach, termed MD-DCCA, could discern between a free channel, a non-802.15.4 interferer (such as WiFi), and 802.15.4 transmissions, thereby achieving DCCA. Unfortunately, in order for transceivers to provide modulation detection, more complex radio circuitry is required. Therefore, most currently available transceivers do not implement this method, and opt instead only for simple energy detection CCA.

This is the case with the Texas Instruments family of IEEE 802.15.4 transceivers, including the CC2420, found in many WSN installations. While the specification for the CC2420 [13] suggests that all CCA modes are supported, this is not the case for modulation detection, where a busy channel is inferred only if a packet is currently being received. Since this requires being able to receive and decode the packet preamble, this is insufficient to implement DCCA.

This was confirmed experimentally using three Tmote Sky nodes. The first was programmed to transmit packets continuously. The other two nodes continuously performed CCA, one using energy detection and one using modulation detection. Two experimental runs were carried out. In the first, sender and receivers use the same Start Frame Delimiter (SFD) while in the second run different SFD are used.

The results are shown in Figure 2. Channel 0 shows the transmitter, a high signal is shown when a packet is in transmission. Channel 1 shows the receiver using modulation detection and Channel 2 shows the receiver with energy detection. The receivers show a low signal when the CCA detects a transmission. Figure 2(a) shows the results when sender and receiver use the same SFD setting while Figure 2(b) shows the result for differing SFD configuration.

It can be seen that for modulation detection to work on the CC2420, the SFD value must match on the transmitter and the receiver. A CCA using modulation detection that would be performed after the packet transmission has begun would result in a clear channel response (as the SFD would not be seen). This shows that modulation detection as-per the IEEE 802.15.4 specification is not

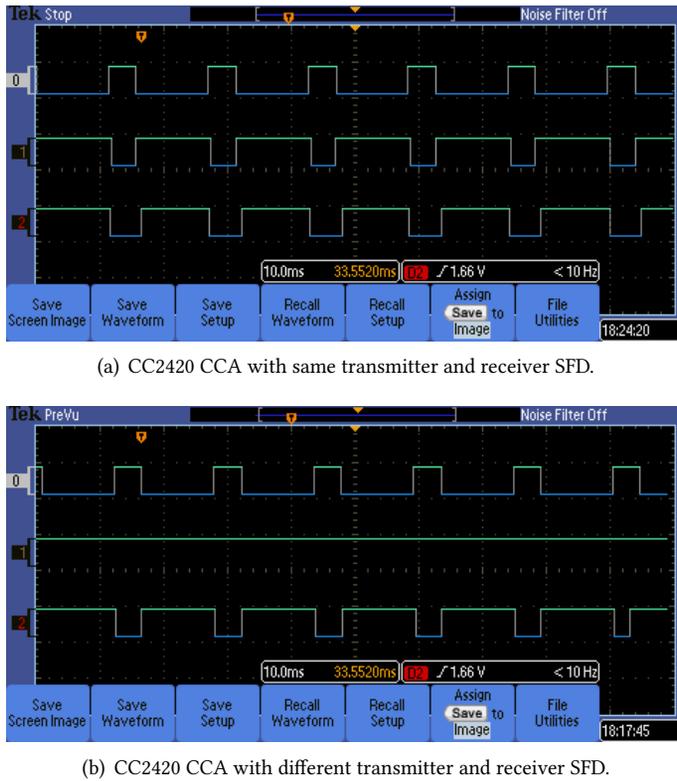


Fig. 2. CC2420 CCA implementations using energy and modulation detection modes. If the value of the SFD at the receiver is changed, modulation detection can no longer detect IEEE 802.15.4 packets

available on the TI CC2420 family. The same observation has been made previously by Petrova et al. [20].

Time Differentiating Clear Channel Assessment (T-DCCA). The different observable characteristics between Physical Layer (PHY) and MAC layers can be leveraged to implement DCCA. For example, the largest 802.11g packet requires only $254 \mu\text{s}$ on-air time, while the largest 802.15.4 packet requires $4224 \mu\text{s}$. Likewise, the Orthogonal Frequency Division Multiplexing (OFDM) used by 802.11n means that the energy on a single overlapping 802.15.4 channel varies throughout the transmission. This is unlike 802.15.4 modulation, which uses Direct Sequence Spread Spectrum (DSSS) and has a more static profile.

WSN nodes can observe these features by recording a Received Signal Strength Indicator (RSSI) trace at high frequency, from which 802.15.4 signals can be identified in the time domain. Hence, this approach is termed T-DCCA. To achieve high accuracy, nodes implementing T-DCCA require a longer listening duration than compared to the standard IEEE 802.15.4 CCA. This increases latency before receivers can react to a DCCA result, and increases the energy consumption of idle listening.

ZiSense [28] is an implementation of T-DCCA which we use for comparison with the P-DCCA approach presented in this paper.

Power Differentiating Clear Channel Assessment (P-DCCA). Building on T-DCCA, P-DCCA, also samples RSSI at high frequency to identify prior-known signal characteristics. However, in order

to reduce the required sampling duration, P-DCCA does not rely on inherent 802.15.4 features, such as spectral profiles and packet durations. Instead, P-DCCA relies on an additional signal component that is modulated by the transmitter, and can be detected by analysing an RSSI trace. This is orthogonal to the data transmission, and acts only to differentiate signals from interference. Since these features are intentionally observable on a smaller timescale, the detection time is reduced compared to T-DCCA.

One implementation of P-DCCA, which we describe in Section 3, achieves this by varying the output power cyclically throughout packet transmission. P-DCCA receivers sample the RSSI register at high frequency, detecting these encoded characteristics within the trace. Signals which lack this feature are assumed to be other interference. This approach has a short detection period, close to the IEEE 802.15.4-standard CCA duration, and thus has a lower idle listening cost compared to T-DCCA.

2.3 Discussion

Traditional energy-based CCA has limitations and we have presented DCCA as a conceptual extension to CCA. DCCA enables us to differentiate interference sources and to implement policies on handling interference.

MD-DCCA would be an efficient solution, however, as this mechanism is not available on most radio chips used today it is desirable to have alternative methods at hand. Both T-DCCA and P-DCCA rely on RSSI features, recorded over time, to identify interference. The former is a passive approach, and relies on features inherent to the IEEE 802.15.4 PHY, and MAC protocol, and therefore requires long sampling durations which reduce energy efficiency. Conversely, P-DCCA is an active approach, which modulates an orthogonal signal feature to all outgoing transmissions. This can be detected during far shorter P-DCCA checks - hence improving energy efficiency. Also, this method allows us to differentiate between two different 802.15.4 networks if required.

The power variation used in P-DCCA reduces the Signal to Noise Ratio (SNR) of the transmission, which in turn reduces the maximum communication distance (See evaluation in Section 6). This presents a tradeoff between P-DCCA and T-DCCA in terms of shorter idle listening and link range.

3 Power Differentiating Clear Channel Assessment (P-DCCA)

In this section, P-DCCA is described in detail, including an implementation on WSN hardware. Our approach is based on varying the output power between two values during packet transmission. Our implementation is based on the common TI CC2420 transceiver, however we believe P-DCCA should be implementable on any IEEE 802.15.4-compliant hardware. An implementation of T-DCCA based on ZiSense [28] is also briefly described. We use this implementation in our evaluation to compare our P-DCCA approach with T-DCCA.

3.1 P-DCCA Mechanism

P-DCCA requires transmission of packets with alternating transmission power. A P-DCCA check must detect this information if present. Within this process the implementation specifics of the RSSI measurement facility on transceiver hardware must be taken into account. The 802.15.4 specification states that CCA detection time shall be equal to eight symbol periods. Hence, a reading of the RSSI register on currently available 802.15.4 transceivers provides an average RSSI measurement over eight symbol periods. Alteration of the transmission power as used for P-DCCA and as shown in Figure 3(a) is perceived as slow increase or decrease of the RSSI at the receiver as an average is computed (see Figure 3(b)).

The timing of transmission power alteration and the algorithm to detect presence of this signature must take this RSSI averaging process into account. Next we discuss transmission and detection

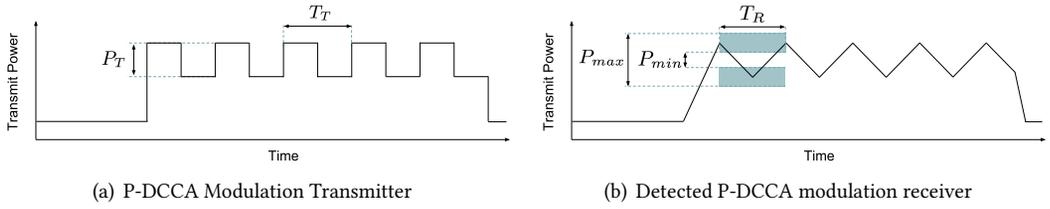


Fig. 3. P-DCCA transmitter power cycle and observed RSSI reading at a receiver node.

Table 1. P-DCCA parameters and values for CC2420 802.15.4 Transceiver.

Parameter	Description	CC2420
P_T	Difference between the two used power levels	5dB
T_T	Transmit power variation period	256 μ s
T_R	Duration of a P-DCCA check	256 μ s
N_R	Number of RSSI samples taken during a P-DCCA check	8
C	Duration of a RSSI sample	32 μ s
P_{min}	Minimum power range of the P-DCCA sample set	2dB
P_{max}	Maximum power range of the P-DCCA sample set	7dB
P_δ	Maximum power difference between two consecutive P-DCCA samples	4dB
N_E	Maximum number of extrema in the P-DCCA sample set	2
τ_{RSSI}	The minimum threshold for each RSSI sample	-75dB

procedures in detail. Parameters governing these mechanisms are given in Table 1. Table 1 also shows settings for these parameters as used within our implementation of P-DCCA based on a TI CC2420 transceiver, which we describe later.

3.2 P-DCCA Signal Transmission

P_T and T_T define the power-cycle of P-DCCA, used during the transmission of P-DCCA modulated packets. Packets are transmitted while alternating between two transmit power settings¹ resulting in a transmit power range of P_T . Each transmit power is used for the same length of time covering the period T_T .

T_T is set to 256 μ s. This is twice the length of the RSSI averaging window, which in most cases is 8 symbol periods (128 μ s). Thus, it is ensured that the maximum and minimum transmission power level used are each fully represented in the RSSI register during a power-cycle (see Figure 3(b)). Aligning the power-cycle duration T_T with the RSSI averaging time ensures that a node performing P-DCCA can observe a signal constantly alternating between minimum and maximum power which simplifies the detection process.

P_T must be large enough to ensure that signal features are reliably discernible to receivers. P_T must be selected such that power variations can be distinguished clearly from natural signal strength variations. P_T must also be minimised such that transmission power remains sufficiently strong at the intended receiver, as reduced transmit power leads to a reduced transmission range.

¹In practical settings the strongest and second strongest available transmission power are used but other power settings are possible too.

3.3 P-DCCA Signal Detection

A simple algorithm is necessary for signal analysis as a fast execution on resource constraint nodes is necessary. The signal analysis must be carried out during a brief CCA check. The wave form as shown in Figure 3(b) must be detected reliably. This can be achieved by simply detecting local power extrema and analysis of power ranges. During P-DCCA the RSSI register is sampled periodically for a period of time T_R . The sampling period must be larger or equal to the power-cycle period T_T to ensure that at least one complete set of power extrema is covered ($T_T \leq T_R$). The collected RSSI *sample set* is then analysed using Algorithm 1.

Algorithm 1 Power Differentiating Clear Channel Assessment (P-DCCA).

```

1: for  $i = 1$  to  $N_R$  do
2:   if  $(s[i] = \text{RSSI}()) < \tau_{\text{RSSI}}$  then break
3:   if  $i = 1$  then return CLEAR
4:   if  $i < N_R$  then return BUSY_INCONCLUSIVE
5:   for  $i=1$  to  $(N_R - 1)$  do
6:     if  $|s[i] - s[i + 1]| > P_\delta$  then return BUSY_OTHER
7:     if  $s[i] > s[i + 1] \wedge \text{slope} \neq \text{SLOPE\_INCREASING}$  then
8:        $\text{slope} \leftarrow \text{SLOPE\_INCREASING}$ 
9:        $\text{counter} \leftarrow \text{counter} + 1$ 
10:    if  $s[i] < s[i + 1] \wedge \text{slope} \neq \text{SLOPE\_DECREASING}$  then
11:       $\text{slope} \leftarrow \text{SLOPE\_DECREASING}$ 
12:       $\text{counter} \leftarrow \text{counter} + 1$ 
13:    if  $(\text{range}(s) < P_{\min} \vee (\text{range}(s) > P_{\max}) \vee (\text{counter} > N_E))$  then
14:      return BUSY_OTHER
15:  return BUSY_PDCCA
  
```

The first two lines in the algorithm fill the sample set s with RSSI values until a single value below the threshold τ_{RSSI} is received, or until N_R samples have been taken. N_R is dictated by the achievable sampling frequency and T_R . If the first RSSI sample is below the threshold τ_{RSSI} , P-DCCA indicates that the channel is free, without taking any more samples. Thus, an unoccupied channel causes P-DCCA to behave identically to the normal CCA method. If N_R samples are collected over the minimum threshold, the algorithm measures these samples against the given thresholds in Table 1. On line 6, the absolute value between consecutive samples is compared against P_δ , and lines 7 through 12 count the number of local power extrema. Finally on line 13, the range of the samples and the number of local extrema are compared against their thresholds P_{\min} , P_{\max} and N_E respectively. A signal passing these thresholds is classified as a valid, P-DCCA modulated 802.15.4 signal.

3.4 P-DCCA Outcome

P-DCCA can have four distinct outcomes:

- (1) *CLEAR*: indicates that the medium is currently free.
- (2) *BUSY_PDCCA*: indicates that a transmission with P-DCCA power modulation was detected.
- (3) *BUSY_OTHER*: indicates that another signal without P-DCCA was detected, such as WiFi, Bluetooth, or another IEEE 802.15.4 device outside the network.
- (4) *BUSY_INCONCLUSIVE*: indicates that the medium is busy but the channel occupier cannot be determined.

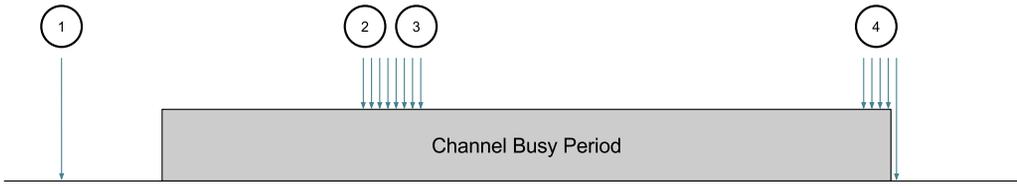


Fig. 4. Possible P-DCCA outcomes: 1) One sample: channel is clear (*CLEAR*) 2) Complete sample set: channel is either *BUSY_PDCCA* or *BUSY_OTHER* 3) Incomplete sample set: channel is busy, but unknown origin: *BUSY_INCONCLUSIVE*

P-DCCA requires N_R RSSI samples, above the threshold, to identify a signal. Therefore, if a P-DCCA check coincides with the end of a busy period, an incomplete RSSI set may be recorded and no source may be definitively identified. This results in a *BUSY_INCONCLUSIVE* result, the interpretation of which is left to the MAC layer. Situations leading to these P-DCCA outcomes are shown in Figure 4.

3.5 P-DCCA Interpretation

Node behaviour after obtaining a P-DCCA result is to be decided by upper layers. *CLEAR* may be treated similar to a clear resulting from a normal CCA. *BUSY_PDCCA* would trigger the back-off procedures designed to coordinate competition for the channel among nodes of the same network. The reaction to *BUSY_OTHER* may depend on knowledge of the deployment area. For example, it might be known that other interference is likely to stem from a co-located WiFi network.

In case of *BUSY_INCONCLUSIVE* the decision may depend on worst-case or best-case assumptions. For example, a prudent node listening to the channel for incoming packets may treat this result as normal 802.15.4 traffic, leaving the radio powered on to receive data, while an energy-conscious node may ignore altogether any interference except confirmed 802.15.4 traffic.

Alternatively, *BUSY_INCONCLUSIVE* results can be avoided altogether by stipulating design requirements on the MAC protocol. Knowing the duration between packet transmissions, two P-DCCA checks can be arranged so that at least one will fall within a packet transmission. Thus, inconclusive results can be ignored entirely. This approach ensures that at least one sample set captures a P-DCCA signal, ensuring reliable operation.

3.6 CC2420 Implementation of P-DCCA

Our implementation and evaluation of P-DCCA is based on the Tmote Sky WSN platform [6]. This platform uses the TI MSP430 MCU and CC2420 radio, which is compliant with the IEEE 802.15.4 PHY. The specific P-DCCA parameters used for the implementation are given in Table 1.

The RSSI register of the CC2420 does not contain an instantaneous representation of the current channel energy. It contains an average over the preceding 8 symbol periods of $128\mu s$ duration. We set $T_T = 256\mu s$. We set $T_R = T_T$ as we decided to use only one power-cycle for detection ($N_E = 2$). Larger T_R could improve detection accuracy but would increase P-DCCA duration which would have an additional energy cost. However, as our evaluation shows (see Section 4) this duration is sufficient to achieve high detection accuracy. We use a power difference of $P_T = 5dB$ as we observed this to be the smallest power difference yielding good detection accuracy. The transmit power alters between $0dB$ and $-5dB$.

The maximum RSSI sampling frequency we were able to achieve on the CC2420 was $33MHz$. To ensure reliable timing with the RSSI sampling window, this was reduced to $31.2MHz$ to synchronise

with every second IEEE 802.15.4 symbol. Based on this, $N_R = 8$ samples are collected during a power-cycle of length T_T . We empirically set $P_{min} = 2dB$, $P_{max} = 7dB$ and $P_\delta = 4dB$ which is tuned to the chosen transmission power difference $P_T = 5dB$ and accuracy of the CC2420 RSSI measurement facility.

P-DCCA is implemented in the Contiki WSN OS [10], where operation of the radio driver strays little from the standard implementation. The function used to transmit a packet blocks until the transmission of a packet has been completed; in P-DCCA, this blocking time is used to modulate the output power. In our measurements, the P-DCCA function call may take up to $260\mu s$, as opposed to the immediate response with normal CCA; this timing component must be accounted for in the implementation of MAC protocols.

3.7 Implementation of T-DCCA

In ZiSense RSSI traces are searched for known IEEE 802.15.4 signatures. ZiSense is designed to improve the wake-up and rendezvous mechanism in WSN MAC protocols: to reduce the false wake-up problem, and improve the resilience of synchronisation packets in protocols such as X-MAC [4]. Although ZiSense was not directly designed as DCCA mechanism, it can be employed in this capacity as representation of T-DCCA and we use it in this work for comparison in our evaluation.

Each ZiSense check listens to the channel for a fixed duration, sampling the RSSI into a buffer. The buffer is analysed and segments are identified as contiguous subsets of RSSI samples when the signal differs from the noise floor. For each segment detected, a feature-set is constructed describing:

- (1) On-air time
- (2) Peak-to-Average Power Ratio (PAPR)
- (3) Inter-Packet Spacing (IPS)
- (4) Under Noise Floor (UNF)

(1) and (3) describe temporal features of the signal, which are typically specific to the MAC protocol. The original authors of ZiSense used TinyOS LPL as the MAC protocol in their evaluation. (2) stems from the modulation used by the transmitter. (4) is a feature unique to interference from electric machinery (i.e. Microwave Ovens), where the signal strength drops below the noise floor.

These feature sets are then passed to a classification algorithm, to classify each segment as either IEEE 802.15.4 or other. In [28], three algorithms are described: *ZiSense-1*, *ZiSense-2*, and *ZiSense-C4.5*.

- *ZiSense-1*: A classifier manually derived from strict interpretation of IEEE 802.15.4 PHY and TinyOS LPL.
- *ZiSense-2*: A more forgiving classifier manually derived to identify segments that have collided with other interference.
- *ZiSense-C4.5*: A classifier build using the C4.5 algorithm, which builds a decision tree classifier from a prior-known dataset - in this case from segments which were identified manually.

Since no implementation of ZiSense is currently available we recreated the ZiSense algorithm offline, based on [28]. Our implementation samples the RSSI register at the same frequency into a buffer on a Tmote Sky sensor node. Once full, these raw RSSI values are sent to the host computer via serial link. The ZiSense classification algorithms described above are then run offline. An offline approach avoided complications in developing embedded WSN software, while still allowing for classification accuracy comparisons.

It has to be noted that a CCA check using ZiSense (a T-DCCA) variant takes much longer than a CCA check using P-DCCA. Longer sample periods are required and more complex computation is necessary compared to P-DCCA. Hence, ZiSense is more costly in terms of energy consumption. On

the other hand, ZiSense does not affect communication range. P-DCCA requires active modification of the transmission signals while ZiSense needs to have a clear understanding of protocol behaviour. Both options have advantages and disadvantages we quantify in our evaluation.

4 ACCURACY EVALUATION

In this section, we evaluate the accuracy of the P-DCCA classification algorithm, and compare it with the ZiSense T-DCCA classification algorithm. We evaluate both DCCA mechanisms in terms of True Positive (TP) and False Positive (FP) rates, these are defined as:

- **True Positive (TP) Rate** - the rate of correct WSN transmission classification by the DCCA algorithm.
- **False Positive (FP) Rate** - the rate of incorrect WSN transmission classification by the DCCA algorithm, in the presence of non-WSN interference.

Accuracy is measured by controlling the interference environment, by injecting either WSN traffic (to measure TP rate), or interference (to measure FP rate). This evaluation considers only the classification accuracy of each DCCA implementation, given a complete RSSI sample set. It is not possible for this comparison to include the underlying sampling mechanism, due to differences in the RSSI sampling approaches. Therefore, *BUSY_INCONCLUSIVE* results are ignored in P-DCCA. As discussed in section 3.4, the MAC layer should be implemented to consider *BUSY_INCONCLUSIVE* results accordingly.

4.1 True Positive (TP) Rate

For this experiment, two Tmote Sky nodes are spaced 4m apart in an unused computer laboratory during quiet office hours. One node transmits packets throughout the experiment, while the other tests the DCCA-variant. The ZiSense detection algorithm relies on temporal characteristics inherent to the applied MAC protocol, which in [28] is TinyOS LPL. Therefore, packets are transmitted 2.9ms apart to emulate LPL traffic. For P-DCCA evaluation these packets are transmitted with power variation. The experiment is repeated five times, during which P-DCCA and T-DCCA are tested for five minutes each.

To evaluate T-DCCA, the offline implementation of ZiSense described in Section 3.7 is used. The duration of a T-DCCA check and its relation to the LPL transmission timing ensures that each T-DCCA check can obtain sufficient data to identify the ongoing WSN transmission.

To evaluate P-DCCA, it is ensured that the P-DCCA check is carried out while a packet transmission is ongoing. To achieve this, transmitter and receiver node are synchronised via a cable connection. Thus, T-DCCA and P-DCCA have both the chance to correctly identify an ongoing transmission within the DCCA check. However, it has to be noted that both DCCA checks have very different time scales (2.9ms compared to 256μs).

The results in Figure 5 show that P-DCCA achieves higher TP rate than all ZiSense classifications. P-DCCA TP rate is 88%, while ZiSense-1, ZiSense-2 and ZiSense-C4.5 have 78%, 86% and 78% respectively. This experiment shows that using P-DCCA, high classification accuracy can be achieved despite a comparably shorter DCCA duration (2.9ms compared to 256μs).

4.2 False Positive (FP) Rate

For this experiment, two Tmote Sky nodes are programmed to act as P-DCCA and T-DCCA receivers, and placed in an unused computer laboratory. The experiment is repeated ten times, each iteration taking five minutes. The experiment takes place during quiet office hours, with minimal external Radio Frequency (RF) activity.

The interference sources are:

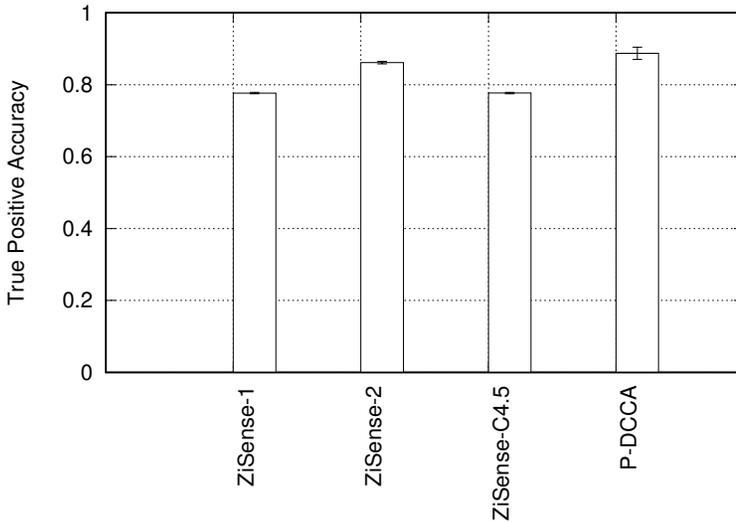


Fig. 5. TP rate of P-DCCA and ZiSense. P-DCCA achieves a better TP rate compared to all ZiSense implementations.

- **WiFi:** An IEEE 802.11 Access Point (AP) and station are placed at opposite corners of the room. Both are connected to a host computer over a wired connection, which acts as the control channel for the experiment. Interference is generated using the [1] DITG tool, 1000-byte UDP packets are transmitted at a uniform random rate as specified. IEEE 802.11 b, g, and n variants are used in the experiments, as configured by the host computer.
- **Bluetooth:** Bluetooth traffic is generated by sending a large file between two devices: a MacBook Pro laptop computer and a Google Nexus 5 Android smartphone.
- **Microwave oven:** Microwave oven interference is generated using a household microwave oven, heating 500ml of water in a pyrex bowl at 800W, replaced at the beginning of each experiment run.

Both nodes continuously call the DCCA function, the outcome of the detection mechanisms is recorded on the host computer. An FP result is recorded whenever an IEEE 802.15.4 packet is detected.

The results are shown in Figure 6. For all interference sources, P-DCCA recorded the lowest FP rate. In most cases, this is followed by ZiSense-1 and ZiSense-C4.5. ZiSense-2 records the worst FP rate.

For IEEE 802.11b interference ZiSense variants have a high FP rate. This is due to the closer observable similarity between IEEE 802.15.4 and 802.11b signals: the slower transmit rate and DSSS modulation causes the packet duration and PAPR to fall within ZiSense thresholds. IEEE 802.11g and n have the lowest FP rate across all DCCA approaches.

This experiment has shown that P-DCCA has a far lower FP rate than ZiSense. However, it has to be noted that P-DCCA can return *BUSY_INCONCLUSIVE*. In this case a FP is avoided but not enough information is available to discern the interferer type. Inconclusive results can be mitigated by applying multiple P-DCCA checks.

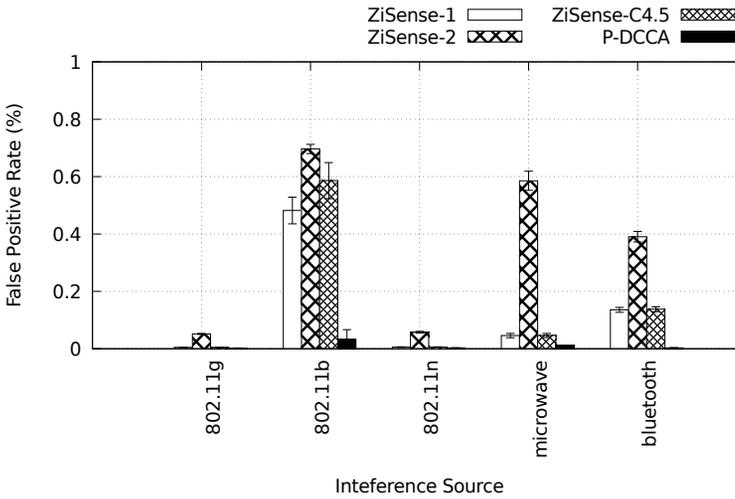


Fig. 6. True Negative accuracy for P-DCCA and ZiSense. For 802.11g, n and bluetooth interference, ZiSense-1, -C4.5, and P-DCCA are closely matched. P-DCCA performs worse in microwave oven interference, while all ZiSense implementations suffer significantly under 802.11b interference.

4.3 Discussion

Our ZiSense results show similar trends relative to the authors' evaluation [28]. ZiSense-2 has the best TP rate but also the worst FP rate. Conversely, ZiSense-1 and ZiSense-C4.5 have better FP rate for a reduced TP rate.

To the best of our knowledge, this implementation of ZiSense matches the original, and we have followed the same approach to measure accuracy. Given that the similar trends between ZiSense implementations have been observed in our results, we believe that the difference in absolute accuracy is due to the different testing environment.

The authors original evaluation did not factor IEEE 802.11b interference, a standard that is now considered obsolete compared to later g, and n, standards. Despite this, we have found that the behaviour of many IEEE 802.11 AP rate selection algorithms - which is manufacturer specific - may fall back to 802.11b PHY in adverse channel conditions. In particular, we observed this to be the case where the AP is vying for channel access under 802.15.4 interference.

In implementing DCCA in a WSN MAC protocol, the implications of a high FP rate must be considered. False wake-ups - where non-802.15.4 signals are classified as incoming WSN traffic, cause increased idle listening and hamper energy efficient operation. When using DCCA, the probability of a false wake-up occurring is a function of the FP rate. *BUSY_INCONCLUSIVE* results can occur as well but can be interpreted as *BUSY_OTHER* to improve energy efficiency.

In P-DCCA, the sampling duration is variable: samples are recorded only whilst the RSSI is above the threshold. Conversely, the ZiSense sampling duration is fixed and much longer (2.9ms for ZiSense compared to a maximum P-DCCA duration of 256 μ s). Furthermore, P-DCCA has the better TP and FP rates.

5 ENERGY CONSUMPTION EVALUATION

In this section, the energy consumption of P-DCCA is evaluated. In particular, we focus on idle listening energy consumption which is the greatest source of energy consumption in most WSN deployments. A node must wake periodically to check for an incoming transmission using a CCA

mechanism which is the dominant energy cost. We analyse this idle listening cost analytically for P-DCCA and compare it with the cost of T-DCCA and normal CCA.

5.1 P-DCCA Energy Consumption Model

We assume that any transceiver activity within the P-DCCA mechanism has the same energy consumption; energy consumption during transceiver startup and during RSSI sampling is the same. This is a realistic approximation for transceivers such as the CC2420 commonly used. Thus, energy consumption of a P-DCCA check depends on the transceiver-on duration T , which we model.

The behaviour of the P-DCCA algorithm described depends on the interference encountered, which must be provided as input to this model. The probability of finding the channel busy at any instant is represented as p ; when busy, the channel is then occupied by an interference signal with fixed duration t . For example, when considering a WiFi interferer an intensity of p and an average WiFi packet length of t can be assumed.

The expected duration T of a P-DCCA check (shown in Equation 1) is the sum of the transceiver start up time, T_{st} ; the duration of the first RSSI sample, which is always taken; and the time taken to carry out the sequence of N_R RSSI samples as described in Algorithm 1. The latter stems from two possible outcomes. Firstly, T_A models the case where the P-DCCA check starts sooner than N_R P-DCCA samples before the end of the interference. Otherwise, fewer samples are taken (T_B).

$$T(t, p) = T_{st} + T_{RSSI} + p \cdot (T_A(t) + T_B(t)) \quad (1)$$

T_A is given in Equation 2, and is the product of the total duration of all RSSI samples: $T_{RSSI} \cdot (N_R - 1)$, and the probability.

$$T_A(t) = (T_{RSSI} \cdot (N_R - 1)) \cdot \left(\frac{t - (N_R - 1) \cdot T_{RSSI}}{t} \right) \quad (2)$$

The remaining interference duration modelled by T_B has duration $t - T_{RSSI} \cdot (N_R - 2)$; this is considered as $(N_R - 2)$ discrete intervals. The probability of each is given by T_{RSSI}/t , and the duration of the subsequent n samples is given by $n \cdot T_{RSSI}$. Therefore, T_B is the sum expected duration of these $(N_R - 2)$ intervals.

$$T_B = \sum_{n=1}^{N_R-2} n \cdot T_{RSSI} \cdot \left(\frac{T_{RSSI}}{t} \right) \quad (3)$$

This model assumes firstly that $t \geq N \cdot T_{RSSI}$: that the duration of the interference signal is greater than the number of RSSI checks in P-DCCA. This is not necessarily true for all types of interference, in which case T represents an upper-bound. Secondly, the model assumes that p and t are independent variables.

Knowing how much power the transceiver consumes when active and the number of DCCA checks necessary (channel check rate) the idle energy consumption using P-DCCA can be computed. The channel check rate and the number of P-DCCA checks necessary at each instance depends on the used MAC protocol.

5.2 LPL Energy Consumption

We now assume TinyOS LPL as WSN MAC protocol to evaluate idle listening energy consumption of P-DCCA, ZiSense as T-DCCA and the classical CCA without any DCCA capability. We use LPL as WSN MAC protocol as ZiSense was particularly designed for this specific protocol.

TinyOS LPL has an inter-packet spacing of $2.9ms$. Thus, for ZiSense a single CCA check with a duration of $2.9ms$ is necessary to check for an incoming transmission. With the assumption

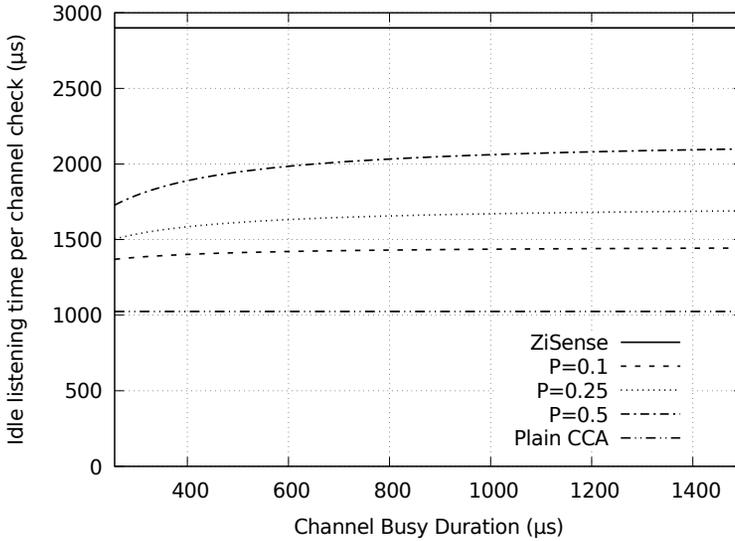


Fig. 7. Energy consumption of P-DCCA and T-DCCA (based on ZiSense) under interference. P-DCCA requires less idle listening time under all channel conditions.

of a minimum packet duration of at least $500\mu s$, 6 CCA checks spaced $500\mu s$ apart, over $3ms$, are sufficient. This channel check behaviour is necessary for DCCA and plain CCA to check for incoming transmissions.

This behaviour can be illustrated using Figure 1. For ZiSense the receiver CCA shown in Figure 1 is performed over a long period of $2.9ms$. For DCCA and plain CCA the receiver CCA consists of 6 CCA checks spaced $500\mu s$ apart, over $3ms$.

ZiSense and plain CCA has a constant energy cost per channel check. However, plain CCA would not be able to infer the nature of the channel occupier and any observation of interference would lead to a false wake-up, contributing significantly to energy consumption; we do not consider this aspect here and include plain CCA only as reference point. P-DCCA has a variable energy cost which depends on the present interference signal.

Based on this, the radio-on time per DCCA check for P-DCCA, ZiSense and plain CCA are shown in Figure 7, for interference conditions described by $p = 0.1, 0.25, 0.5$ and variable duration t .

Plain CCA has the same energy cost as P-DCCA when interference approaches zero. P-DCCA has an energy cost which is much lower than that of ZiSense. Given that P-DCCA was shown in Section 4 to have at least similar detection accuracy as ZiSense P-DCCA will provide better energy efficiency when considering DCCA as receiver mechanism.

6 RANGE EVALUATION

P-DCCA requires transmission power variation which means that a signal cannot be transmitted continuously with full power. Hence, it has to be assumed that the achievable transmission range is reduced. In this evaluation we evaluate the impact of transmit power variation on the achievable communication distance.

The transmission power variation used by P-DCCA reduces the signal strength and SNR of the received signal. This reduces the ability of the IEEE 802.15.4 receiver to correctly decode the incoming signal, leading to an increased Packet Error Rate (PER) for a given link. Since signal

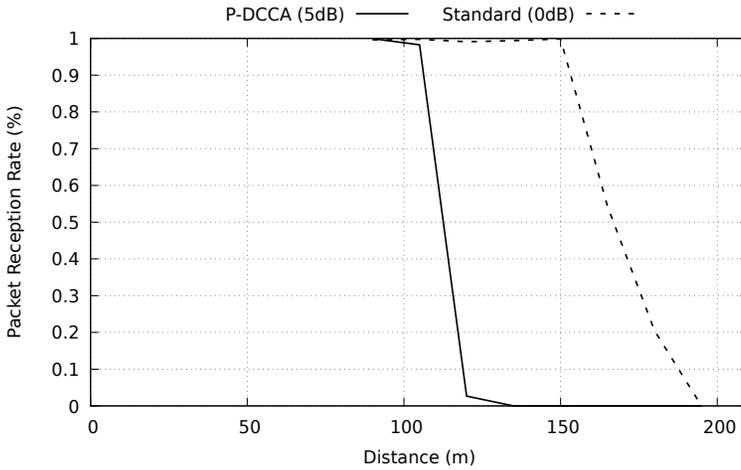


Fig. 8. Link distance for P-DCCA and without power variation. P-DCCA power variation leads to a reduction of communication distance. P-DCCA achieves 100% PRR up to 105m compared to 150m without P-DCCA.

strength loss is a function of the distance between sender and receiver, P-DCCA links will have a shorter communicable distance, compared to uniform transmission power.

We use two TelosB nodes configured as sender and receiver; the former is programmed to transmit 90 byte packets at a rate of 16 packets/second; the latter records each packet received to a buffer in RAM. These results are then retrieved by a host computer after the experiment. The experiment takes place outside in an empty sports field, and the distance between the nodes is varied from 90m to 180m, in increments of 15m. PRR is recorded for 3 minutes, for each distance. For each increment, the PRR is calculated. The transmitter node does not implement CCA checks or retransmissions, and neither node duty cycled the radio. Both nodes are elevated 75cm above the ground to ensure line of sight.

Two P-DCCA configurations are used: $P_T = 0dB$ which is the uniform transmission power; $P_T = 5dB$ which is the setting used for the CC2420 implementation. The results are shown in Figure 8.

PRR follows the same pattern with both transmission powers: 100% PRR up to a cutoff point, beyond which no packets are received. The receiver can compensate bit errors up to a point where the packet cannot be successfully reconstructed. The transitional region between 100% PRR and 0% is often very small as in this experiment (see Petrova et al. [19]). For $P_T = 5dB$, this distance is 105m. By contrast, using the maximum uniform transmission power, $P_T = 0dB$, this range is extended to 150m. Therefore, P-DCCA in this implementation incurs a reduction in link range of approximately 30%.

The reduced link range is the main drawback of using P-DCCA. In a large, multi-hop network, more hops may be needed to communicate, increasing energy consumption and offsetting the benefits of P-DCCA. Otherwise, if nodes are too sparsely deployed, P-DCCA may fragment the network and prevent communication entirely. P-DCCA may therefore be better suited to either smaller networks, with few nodes, or large, multi-hop networks, with many possible links.

However, when considering the design of sender-initiated asynchronous MAC protocols, it becomes apparent that the link performance is not the only parameter determining maximum link distance. Receivers implementing these MAC protocols periodically sample the channel energy using CCA checks: if the set CCA threshold is exceeded, an incoming packet is inferred, and the

radio remains powered on to receive a packet. Otherwise, the radio is powered off, until the next wake-up sequence. Therefore, for a packet to be received it is necessary that the RSSI exceeds the CCA threshold. Lowering the threshold improves detection of incoming transmissions (and range) while increasing the rate of false wake-ups. For example, Oppermann et al. [18] have investigated CCA threshold selection to balance PRR and energy consumption.

Even though it might be generally possible to receive a packet at a specific distance, the receiver may not be able to clearly detect the incoming transmission using CCA. Thus, the limiting factor of maximum link distance in sensor networks may be detection of the incoming transmission rather than the ability to decode it successfully.

7 P-DCCA APPLICATION

To evaluate the benefit of P-DCCA in practice, we implemented it in a popular WSN MAC protocol: ContikiMAC. ContikiMAC with P-DCCA is then evaluated in a variety of testbed and practical deployments and the achievable network performance is evaluated and compared with plain ContikiMAC. The presented evaluation is specific to ContikiMAC; however, similar performance improvements are to be expected when applying P-DCCA to other WSN MAC protocols.

To include P-DCCA in a WSN MAC protocol it is necessary to replace the sender and receiver based CCA mechanism with the P-DCCA mechanism. It has to be taken into account that P-DCCA requires additional time compared to the standard CCA (see Section 3). The additional time required depends on the used transceiver hardware and in many cases this additional required time does not require modifications to the MAC protocol. When transmitting messages the power modulation must be included.

7.1 P-DCCA in ContikiMAC

ContikiMAC [9] resembles other WSN MAC protocols (see section 2) which use CCA for receiving and transmitting. To save power, ContikiMAC nodes keep the radio in a powered-down sleep state, and periodically listen for incoming packets once every duty cycle. Transmitters continuously transmit a strobe sequence back-to-back to the recipient, listening in between each packet for an acknowledgement. The operation of ContikiMAC is depicted in Figure 9.

To listen for incoming packets, each node in the network uses two CCA spaced $0.5ms$ apart; a busy channel detection from either causes the radio to be left powered-on to receive the next subsequent packet from the transmitter. Likewise, senders must check the channel is free using six CCA before transmitting, and one CCA between packet strobos - a single busy channel detection will cause the transmission to stop.

To reduce unnecessary transmissions when the receiver is asleep, Phase Lock (PL) is an optimisation in ContikiMAC which learns the wake-up times of neighbouring nodes. Future transmissions are then delayed until just before the receiver is expected to wake.

P-DCCA allows us to improve ContikiMAC's behaviour in interference environments as it enables us to implement fine-grained reaction to different interferer types. We decide to augment ContikiMAC with the following simple DCCA behaviour:

- **Transmitter DCCA:** Transmissions are only stopped in response to detecting 802.15.4 traffic, ignoring other channel interference.
- **Receiver DCCA:** The radio is only powered on to receive data after detecting 802.15.4 traffic, ignoring other channel interference.

ContikiMAC senders persist with transmissions after detecting interference, motivated by the possibility that the target node may still correctly receive the packet over the interference. This may be due to variation in the interference signal strength throughout the network, or due to the

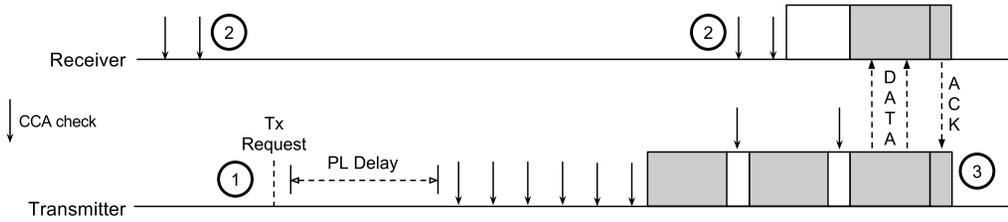


Fig. 9. Normal Operation of ContikiMAC: 1) Transmit request is followed by Phase-Lock delay, and CCA check before transmitting. 2) Periodic Receiver CCA check detects incoming packet, entering receive-sequence. 3) After data received, ACK transmitted, and packet strobes stop.

short channel occupation time of the interferer. Transmitters only back off if 802.15.4 traffic is detected within a CCA before transmission.

ContikiMAC receivers avoid listening to the channel for incoming packets unless 802.15.4 traffic has been detected - reducing false wake-ups and improving energy efficiency. While inconclusive results are ignored, the risk of ignoring valid 802.15.4 packets is eliminated in the design of ContikiMAC: the $0.5ms$ spacing between CCA checks ensures that at least one CCA check will not fall at the end of a packet in the strobe sequence (see Figure 9).

In our evaluation we compare network performance of plain ContikiMAC and ContikiMAC with P-DCCA extension. In all setups the same network and interference configuration is used for ContikiMAC and ContikiMAC with P-DCCA.

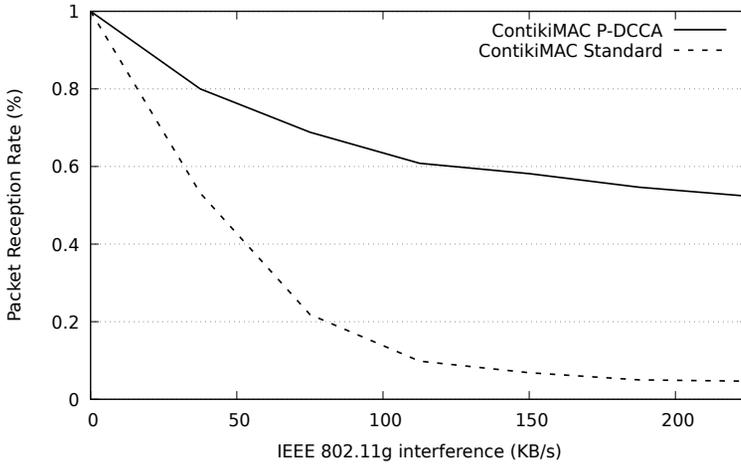
7.2 Experiment 1: Single WSN Transmitter

In the first experiment, the link performance and energy efficiency of ContikiMAC is measured in controlled interference conditions. Two Tmote Sky are placed in opposite corners in an unused office, spaced $6m$ apart. The nodes are connected to a host computer over a USB connection, used for reprogramming and communication. In the same office, an IEEE 802.11g access point and station are placed in opposite corners, and are connected to the host computer over a wired connection. Interference is generated using the D-ITG traffic generation tool [1], sending UDP traffic with varying intensity. The set traffic rates were achieved with present 802.15.4 traffic as the channel was not fully saturated. The experiment takes place during quiet office hours with reduced wireless background traffic in the building. WiFi channel 11 and IEEE 802.15.4 channel 22, which were found to be the quietest overlapping channels in the environment, are used for the experiment. 90-byte packets are sent at a rate of 4 packets per minute without retransmissions. The following performance metrics are recorded:

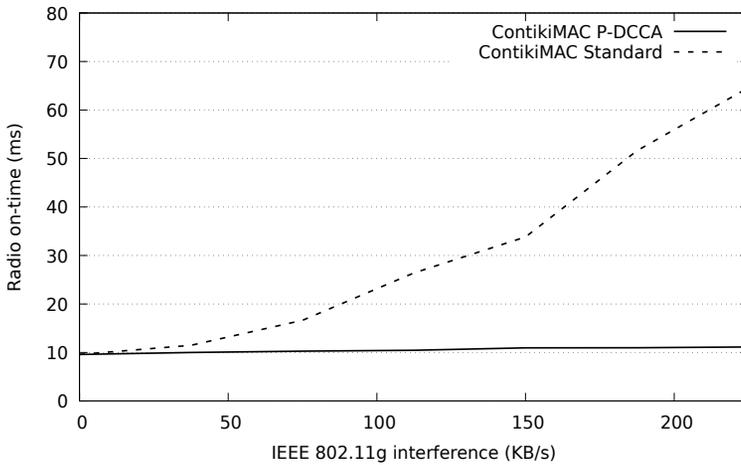
- **Packet Reception Rate (PRR):** PRR is a reflection of the link performance, and is the ratio of successful packet transmissions to total attempts.
- **Radio-on Time Per Packet Received (RoT):** RoT is used to measure the energy efficiency of ContikiMAC under interference. It is the time the transceiver is in an active state divided by the number of successfully received packets.

PRR and RoT are recorded at the receiver during the experiment. Each interference level is run for five minutes. The results are shown in Figure 10.

Figure 10(a) shows that the PRR of ContikiMAC is markedly improved using P-DCCA. Under the heaviest interference tested, standard ContikiMAC PRR falls below 5%, while the P-DCCA variant achieves above 50%. The graph shows that the improvement of P-DCCA over standard ContikiMAC



(a) Packet Reception Rate



(b) Radio-on time

Fig. 10. ContikiMAC with standard CCA and P-DCCA. P-DCCA significantly improves packet reception rate and energy efficiency under interference.

becomes greater as interference increases. This is because as interference increases, the probability of a collision with ContikiMAC CCA increases. In case of standard ContikiMAC a collision results in an aborted transmission which leads to a PRR reduction. In case of ContikiMAC with P-DCCA the transmission is carried out (unless it is the case of a false negative P-DCCA classification) which is then often successful.

In Figure 10(b), the radio-on time per packet received increases proportionally with the interference rate. This is because as interference increases, PRR falls - increasing the energy expenditure per packet. Also, false wake-ups increase, which increase idle listening. In both cases, 10ms is the minimum achieved on-time, this reflects the guard time when a sender begins transmitting packets, before the receiver is expected to wake up. As interference increases, standard ContikiMAC shows

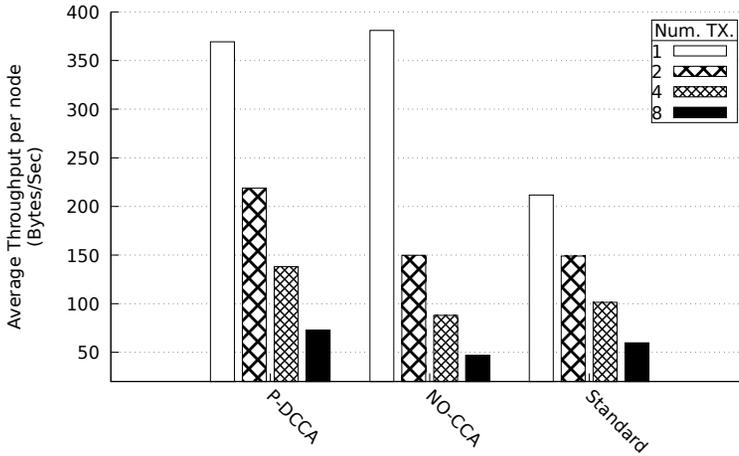


Fig. 11. ContikiMAC Evaluation with multiple transmitters under WiFi interference. P-DCCA provides the greatest throughput compared to standard ContikiMAC and NO-CCA.

significantly worse performance, measuring $65ms$ under heavy interference, while the radio-on time of P-DCCA rises to only $12ms$.

This experiment has shown that a simple DCCA policy on top of the P-DCCA mechanism significantly improves network performance. PRR is improved while energy consumption, expressed via RoT is reduced. For the highest measured interference level PRR is improved ten-fold, while RoT is reduced by 82%.

7.3 Experiment 2: Multiple WSN Transmitters

The previous experiment affirmed the benefits of P-DCCA in a single transmitter environment, where only one ContikiMAC node is transmitting. In this case, any interference detected is known to have originated from outside the network, such as from WiFi interference. However, in interference environments with multiple transmitters, CCA collisions may be due to either interference, or another WSN transmitter. In these cases, channel arbitration can be aided by P-DCCA. For example, upon collision with a WiFi signal, the more optimal approach in our implementation is to persist with the transmission. Conversely, collision with another ContikiMAC packet should result in the back off behaviour used within the WSN.

In this experiment, an IEEE 802.11g network generates interference at a fixed rate of $37.5KB/s$. Sensor nodes use the ContikiMAC Carrier Sense Multiple Access (CSMA) to handle retransmissions, initiating a random back-off after every unsuccessful transmission attempt. On each node, upon an acknowledgement being received or a timeout, a new transmission is initiated - attempting maximum throughput. The average throughput per node is used as evaluation metric.

In each experiment, one, two, four and eight Tmote Sky nodes are used. As well as standard and P-DCCA ContikiMAC, a third derivative is included: NO-CCA, where no CCA checks are conducted either before, or during transmission. In a single transmitter use case, this would be advantageous, since the only source of interference is guaranteed to have originated from outside the network, and an aggressive policy will likely not have a negative impact on the network. This is not the case in a multi-transmitter use case however, since interference may be due to environmental noise or another device in the same network. The results of this experimental run are shown in Figure 11.

The results show that in the case of one transmitter, NO-CCA slightly outperforms P-DCCA. This is due to false positives in P-DCCA - incorrectly detecting WiFi interference as 802.15.4 packets and backing off. With multiple transmitters however, P-DCCA outperforms both NO-CCA and standard ContikiMAC, achieving better average throughput per node. This is due to collisions with other transmitters being avoided, but nodes persisting when faced with WiFi interference.

This experiment has shown that the P-DCCA mechanism significantly improves channel arbitration in an interference environment. For example, when using 4 concurrent transmitters P-DCCA ContikiMAC improves throughput per node by 36% when compared with standard ContikiMAC.

7.4 Experiment 3: Testbed Deployment

Implementing P-DCCA with simple interferer-detection policies has been shown to reduce the energy costs and improve the PRR for individual links. The performance of P-DCCA in the context of a full network deployment (including routing protocol and multi-hop links), is evaluated next using a large scale WSN testbed.

The WISEBED [7] testbed at the University of Lübeck is used. This testbed is located on the 2nd floor of an office building, and consists of 162 nodes arranged in clusters of three. Each node is connected to a host laptop, and the testbed is coordinated over an ethernet backend, which allows for node reprogramming. To aid network configuration, all of the nodes have pre-allocated MAC addresses. For this experiment, only the TelosB nodes in the testbed are used.

All nodes are programmed with the Routing Protocol for Low-Power and Lossy Networks (RPL) routing protocol, which establishes an acyclic graph from a sink node to each node in the network. Each node then has a single parent, to forward data towards the sink, and a number of children, for downstream traffic. As RPL is used, the topology is not static and routing paths are subject to changes. The IPv6 protocol stack is used to handle packet forwarding and address assignment. The default Contiki CSMA behaviour is used to handle retransmissions, with an exponentially increasing back-off and a maximum retry limit of three.

Within the 49-node network, eight nodes are configured as sources. These generate a 60-byte packet every 30 seconds, sent to a single sink node located at one end of the deployment. The remaining nodes are part of the network, forwarding packets as required to the sink. The wakeup frequency of all nodes in the network was set to 8Hz.

It was necessary to generate repeatable and reliable interference under controlled parameters in the testbed. To achieve this, five of the TelosB nodes were programmed to simulate WiFi traffic, as described in JamLab [3]. These nodes used the test transmission mode of the CC2420, whereby pseudo-random data is transmitted continuously on the same IEEE 802.15.4 channel. The nodes alternate between maximum and minimum transmission power, to simulate packetised IEEE 802.11g traffic. The *on* duration of the interference was $577\mu\text{s}$, to simulate 1500-byte packet communication, including IEEE 802.11g RTS/CTS and acknowledgement. The *off* duration, reflecting the spacing between simulated IEEE 802.11g packets, was calculated randomly over a time window that is changed to throttle the degree of interference. This approach does not simulate the IEEE 802.11g MAC protocol, and does not coordinate between simulated interference. As a consequence, the degree of interference (which is used as the independent variable in this experiment) is per-interferer, and is not the sum of all interference during the experiment. This approach allows for an evaluation of P-DCCA over a multi-hop network in the presence of an interference source. In JamLab [3], the authors showed that this approach is able to achieve high accuracy of WSN performance compared to the emulated interferer. The arrangement of sink, sources, other nodes, and interferer nodes in the testbed are shown in Figure 12.

The source and sink nodes report each packet transmission and reception event respectively. This is used to calculate the number of received packets at the sink: $P_{Received}$, and the number

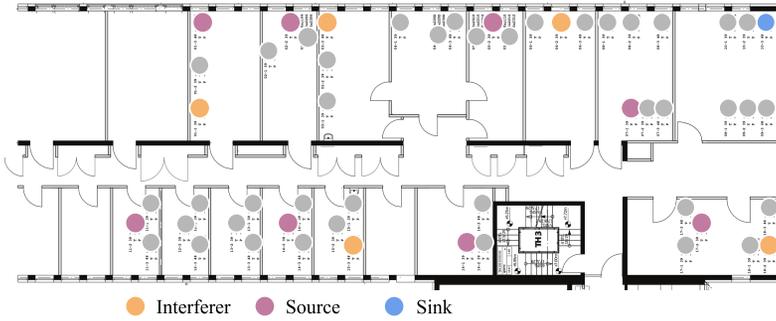


Fig. 12. 54-node Wisebed Deployment in Lübeck, consisting of IEEE 802.11 interferer, source and sink nodes.

of packets sent from the n th source node: P_n . From this, the average PRR from N source nodes is calculated as:

$$PRR_{Average} = \frac{P_{Received}}{\sum_{n=1}^N P_n}$$

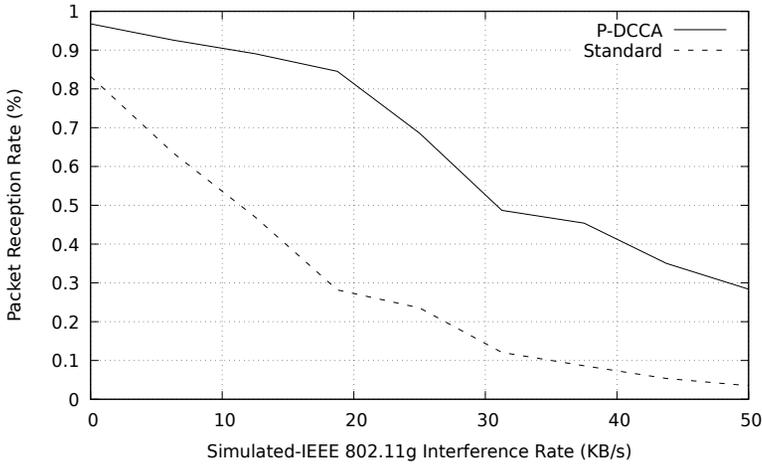
Also, all nodes in the network periodically reported the RoT of each node, every ten seconds. This is used to evaluate the energy efficiency of the network, in the same way as in the first experiment. The average RoT is calculated across all nodes in the network. P-DCCA and standard ContikiMAC variants are tested in 12 minute iterations, for each interference level. The experiment is repeated four times. The results are shown in Figure 13.

The PRR results (Figure 13(a)) are similar to the results obtained in the first experiment. The ContikiMAC P-DCCA variant is less affected by interference than standard ContikiMAC. In this experiment, however, P-DCCA also suffers severe packet loss under high interference rates. This may be due to the cumulative reduction in PRR which is felt across all links on a path - as opposed to the affect on an individual link as measured previously. Also, this experiment simulated interference originating from multiple IEEE 802.11 interferers, as opposed to a single, albeit higher power, interferer. Nevertheless, P-DCCA ContikiMAC clearly outperforms standard ContikiMAC in all interference conditions.

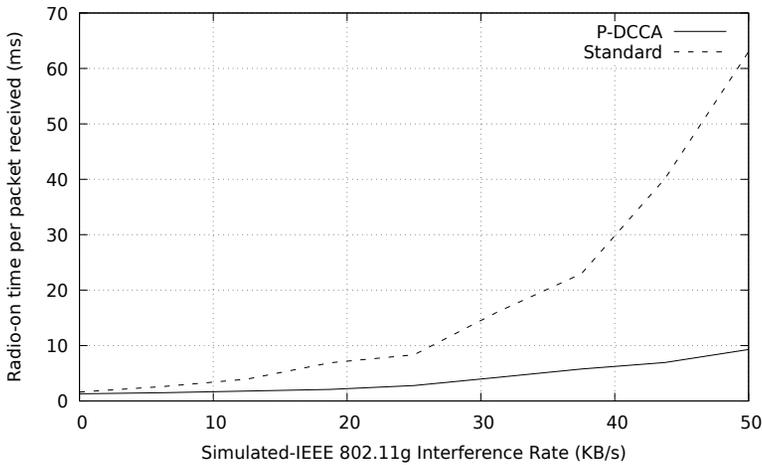
The energy consumption measured via RoT (Figure 13(b)) shows similar trends to earlier experiments. The baseline under no interference is measured as 1.3ms. This is lower than the RoT measured for a single link (as in figure 10(b)), as this is averaged across all nodes in the network - including nodes that do not participate in packet forwarding. As interference increases, the RoT increases drastically with standard ContikiMAC. DCCA mitigates this affect. This is due, in part, to the reduced rate of false wake-ups caused by collisions with interference, and also due to increased PRR with P-DCCA. As before, in this larger experiment, the energy efficiency of P-DCCA is less impervious to interference than in the previous smaller experiments.

These results confirm that P-DCCA benefits link quality and energy efficiency, on an individual link level, and also in large multi-hop networks. Importantly, the reduced transmission range stemming from P-DCCA power modulation does not impair packet delivery. This is due to either link availability or quality being relatively unimpaired by this power modulation, or whose affects are negligible in large networks. Consequently, these results show that the drawbacks of employing P-DCCA are far outweighed by the benefits, in this case.

This experiment has shown that the P-DCCA mechanism significantly improves network performance. PRR is improved while energy consumption, expressed via RoT is reduced. For the highest



(a) Packet Reception Rate



(b) Radio-on time

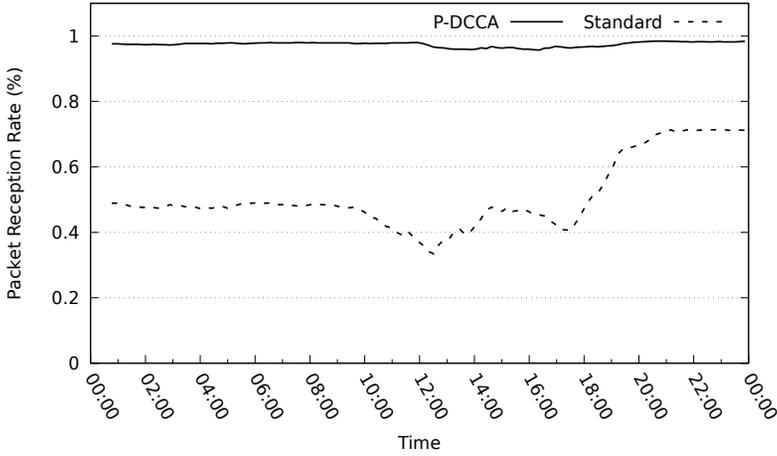
Fig. 13. Energy efficiency and PRR of ContikiMAC and P-DCCA in a large-scale deployment. Results show P-DCCA achieves lower energy consumption and higher packet delivery under interference.

measured interference level PRR is improved seven-fold while RoT is reduced by 85%. Reduced communication range due to the power variation has no negative impact in a relatively dense network setting such as the WISEBED testbed.

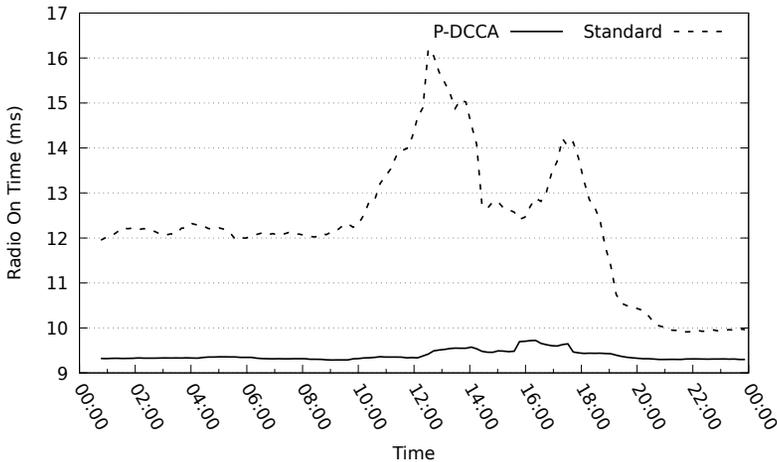
7.5 Experiment 4: Office Deployment

To evaluate P-DCCA over longer durations in an uncontrolled, more realistic environment we used a small office deployment. Two Tmote Sky nodes are placed at opposite ends in a busy office environment, with frequent WiFi interference from nearby laptops and smartphones. The transmitter attempted to transmit packets at a fixed rate of 4 packets per second. Two variants are compared: standard ContikiMAC and ContikiMAC with P-DCCA, each running on both nodes for

five minute intervals. The experiment lasts over 24 hours, and as before, PRR and RoT are recorded. The results of this experiment are shown in Figure 14.



(a) Packet Reception Rate



(b) Radio-on time per packet received

Fig. 14. PRR and Radio-on time of ContikiMAC with and without P-DCCA in a busy office environment. Results show that P-DCCA improves network and energy efficiency throughout the experiment.

The results mirror earlier experiments: P-DCCA improves link performance and node efficiency in ContikiMAC under local RF interference. At peak office hours during this experiment, PRR was improved by up to 180%, and energy consumption reduced by up to 40%.

8 RELATED WORK

The issue of coexistence between 802.15.4 and other devices sharing the radio spectrum is widely established, leading to an assortment of detection, classification and mitigation methods. In particular, 802.11 has been the focus of previous coexistence work, due to its increasing prevalence

in home and industrial automation, medical and sensing technologies - domains popular with 802.15.4. Hauer et al. [11] have shown that WiFi interference is a main cause of packet loss in 802.15.4 networks. The underlying reasons behind this coexistence issue are discussed by Liang et al. [15], asserting that insensitivity to 802.15.4 transmissions and disparate timing parameters disadvantage 802.15.4 nodes and contribute to reduced network performance.

To mitigate the effects of interference on packet loss in WSN, Tang et al. present a solution based on CCA threshold adaptation [23]. Under WiFi interference, the authors show that CCA collisions are reduced by increasing the CCA threshold, thus improving packet delivery rate in the WSN. The authors present a solution that adaptively sets the CCA threshold based on the rate of transmit buffer overflows in a node. This approach is based on ZigBee, which has only one CCA check before transmitting. This is not the case for many WSN MAC protocols, which have multiple CCA per transmission.

Sha et al. similarly consider the CCA threshold in order to mitigate false wake-ups caused by interference [22]. The authors present AEDP, which attempts to raise the receiver CCA threshold in order to reduce false wake-ups, while keeping the threshold low enough however to ensure valid packets are still detected. In order to adapt to different environments, AEDP seeks this optimisation at runtime.

In both cases, these approaches rely on RSSI of interference to distinguish from WSN packets, which is not always guaranteed to be the case. This is not the case with P-DCCA, which modulates the transmission power of sent packets, which can then be detected by other WSN receivers.

Tang et al. present Interference Aware Adaptive Clear Channel Assessment (IAACCA), which more proactively contends for channel access by replacing the standard CCA [24]. Instead of a single CCA check, the channel is sampled continuously until found to be clear. IAACCA is shown to reduce packet loss under WiFi interference compared to standard CSMA mechanism. In the context of this work, IAACCA offers a policy decision after collision with interference, whilst P-DCCA is a replacement for the standard CCA. These works are therefore compatible, and may offer benefits if used in parallel.

Zheng et al. describe ZiSense [28], an active scanning technique in duty cycling MAC protocols to reduce false wake-ups. Similar to P-DCCA, ZiSense samples RSSI at high frequency, listening for timing and spectral characteristics indicative of 802.15.4. Based on these features, ZiSense presents one approach to realising DCCA, which we referred to as T-DCCA in Section 3.7 where it is discussed. By contrast, P-DCCA does not rely on signal characteristics inherent to 802.15.4 to detect incoming traffic. It instead modulates an identifiable signal to the output power of the transmitter, which requires less radio-on time to detect.

The accuracy of ZiSense and P-DCCA is evaluated empirically in Section 4, and the energy consumption of both is compared theoretically in Section 5. P-DCCA is shown to achieve greater accuracy, while requiring less listening time - hence further reducing the energy cost of idle listening.

Tang et al. [23] evaluates the available 802.15.4 CCA modes, energy thresholds and packet loss in the presence of WiFi interference. An adaptive method is proposed to set the energy threshold to achieve optimum performance. Our work goes further than modification of CCA thresholds and an entire new CCA method is proposed.

Detecting and classifying interference has featured in literature to permit deployment planning and direct mitigation techniques [2, 5, 27–29]. These techniques scan the channel over time and observe temporal and spectral indications of heterogeneous traffic. Reaction time is typically in the order of milliseconds or seconds, permitting only per-link countermeasures and infrequent samples to save energy. P-DCCA is not designed to classify environmental interference. Rather, to infer in real time the nature of present channel usage, replacing standard CCA and permitting

interference-specific responses for each transmission. We focus on shortening the detection time without sacrificing accuracy, differentiating only between 802.15.4 and non-802.15.4 interference. We find this to be sufficient for mitigating interference.

An experimental comparison with interference classification methods would be frivolous. Nonetheless, comparing the results of our P-DCCA evaluation in Section 4 with these approaches, suggests comparable accuracy in detecting 802.15.4 transmissions.

Spectral avoidance has featured in literature as a mitigation approach to interference, ensuring coexistence by avoiding collisions entirely [17, 26]. While effective in some situations, this method is ineffective in crowded circumstances, as free channels may become a scarcity. Liang et al. [15] describe how to bolster each packet's resilience to the effects of interference through embedding multiple packet headers and by employing forward error correction. An Automatic Repeat Request scheme for retransmitting partially damaged packets is explored by Hauer et al. [12]. By scanning the RSSI at high frequency during packet reception, spikes from local interference are associated with corruptions in the packet. Our work is orthogonal to these aforementioned works, permitting parallel use to counter interference.

The benefits of a Coexistence Aware Clear Channel Assessment (CACCA) are explored by Tytgat et al. [25], followed by a CACCA evaluation using a Software Defined Radio (see [8]). In this existing work WiFi nodes are equipped with the ability to detect different network types while in our work we consider a CCA extension of 802.15.4 devices. Our proposed DCCA method requires no special hardware, operating on commodity sensor nodes.

In our previous work we have shown that DCCA [14] can help in general to improve network performance. However, in this previous work we have not detailed a mechanism such as P-DCCA that can be used to implement DCCA.

9 CONCLUSION

Given the current pace with which wireless devices are deployed network coexistence is an issue that must be taken into account when designing WSNs and wireless networks in general. DCCA is an effective building block for the implementation of coexisting networks. In this paper we have described and evaluated P-DCCA, a novel DCCA method implementable on current off-the-shelf WSN hardware. We contrasted P-DCCA with the alternative options of MD-DCCA and T-DCCA (using ZiSense as T-DCCA implementation).

MD-DCCA could provide a fast and accurate interference detection. Unfortunately, MD-DCCA is not available on commonly used IEEE 802.15.4 transceivers such as the TI CC2420 (and other models of this family) found in most WSN installations. T-DCCA and P-DCCA can be implemented on existing transceiver models. The interference detection capability of P-DCCA is better than that of T-DCCA in terms of TP and FP rates. Also, the sampling duration during a CCA is much longer for T-DCCA than for P-DCCA ($2.9ms$ for ZiSense compared to a maximum P-DCCA duration of $256\mu s$) resulting in a much better energy efficiency of P-DCCA. To achieve this result P-DCCA requires power modulation of transmissions which result in a small reduction of communication range while T-DCCA does not require a change in transmission behaviour. Also, it would be more challenging to implement P-DCCA in environments where nodes should make use of adaptive transmission power control as, for example, proposed by Lin et al. [16]. T-DCCA would be able to operate in mixed interference environments where the WSN is subject to interference from other 802.15.4 networks and WiFi networks. T-DCCA would here be able to distinguish other 802.15.4 and WiFi interference while P-DCCA would only be able to detect interference (unless the interfering 802.15.4 network uses also power modulation). Although this is a limitation of P-DCCA, we believe that in most deployments interference comes from coexisting WiFi networks. T-DCCA also has

specific detection limitations; for example, T-DCCA has difficulties distinguishing IEEE 802.15.4 and 802.11b transmissions.

In our experiments we used ContikiMAC as an example MAC protocol in order to show the benefits of P-DCCA. P-DCCA achieved energy efficiency in both small, single-hop as well as larger, multi-hop testbed deployments. The former saw packet reception rate improve ten-fold, and energy efficiency improve by over 80% under heavy WiFi interference. These improvements were achieved using simple policies which may not be optimal; better policies to react on P-DCCA outcomes may improve network performance even further.

P-DCCA is not designed to classify interference, rather to discern incoming transmissions from other noise, to achieve high accuracy without sacrificing energy efficiency, nor swaying too far from the standard CCA paradigm. One of our next steps will include the design of improved DCCA reaction policies. Another avenue of future work will be the integration of P-DCCA with other MAC protocols. The work has shown that DCCA is beneficial and we have demonstrated that P-DCCA is a valid implementation option.

ACKNOWLEDGMENTS

This work is partly funded by the Centre for Global Eco-Innovation, part financed by the European Regional Development Fund.

REFERENCES

- [1] Stefano Avallone, S Guadagno, Donato Emma, Antonio Pescapè, and Giorgio Ventre. 2004. D-ITG distributed internet traffic generator. In *Quantitative Evaluation of Systems, 2004. QEST 2004. Proceedings. First International Conference on the*. IEEE, 316–317.
- [2] Bastian Bloessl, Stefan Joerer, Fabian Mauroner, and Falko Dressler. 2012. Low-cost interferer detection and classification using TelosB sensor motes. In *Proceedings of the 18th annual international conference on Mobile computing and networking*. ACM, 403–406.
- [3] Carlo Alberto Boano, Thiemo Voigt, Claro Noda, K Romer, and Marco Zúñiga. 2011. Jamlab: Augmenting sensor network testbeds with realistic and controlled interference generation. In *Information Processing in Sensor Networks (IPSN), 2011 10th International Conference on*. IEEE, 175–186.
- [4] Michael Buettner, Gary V Yee, Eric Anderson, and Richard Han. 2006. X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks. In *Proceedings of the 4th international conference on Embedded networked sensor systems*. ACM, 307–320.
- [5] Kaushik R Chowdhury and Ian F Akyildiz. 2009. Interferer classification, channel selection and transmission adaptation for wireless sensor networks. In *Communications, 2009. ICC'09. IEEE International Conference on*. IEEE, 1–5.
- [6] Moteiv Corporation. 2005. Tmote Sky Ultra low power IEEE 802.15. 4 compliant wireless sensor module. *Datasheet: <http://www.sentilla.com/pdf/eol/tmote-skydatasheet.pdf>* (2005).
- [7] Geoff Coulson, Barry Porter, Ioannis Chatzigiannakis, Christos Koninis, Stefan Fischer, Dennis Pfisterer, Daniel Bimschas, Torsten Braun, Philipp Hurni, Markus Anwander, et al. 2012. Flexible experimentation in wireless sensor networks. *Commun. ACM* 55, 1 (2012), 82–90.
- [8] Peter De Valck, Lieven Tytgat, Ingrid Moerman, and Piet Demeester. 2013. Coexistence Aware Clear Channel Assessment. In *Wireless Sensor Networks*. Springer, 165–178.
- [9] Adam Dunkels. 2011. The contikimac radio duty cycling protocol. (2011).
- [10] Adam Dunkels, Bjorn Gronvall, and Thiemo Voigt. 2004. Contiki-a lightweight and flexible operating system for tiny networked sensors. In *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*. IEEE, 455–462.
- [11] Jan-Hinrich Hauer, Vlado Handziski, and Adam Wolisz. 2009. Experimental study of the impact of WLAN interference on IEEE 802.15. 4 body area networks. In *Wireless sensor networks*. Springer, 17–32.
- [12] Jan-Hinrich Hauer, Andreas Willig, and Adam Wolisz. 2010. Mitigating the effects of RF interference through RSSI-based error recovery. In *Wireless Sensor Networks*. Springer, 224–239.
- [13] Texas Instruments. 2006. CC2420: 2.4 GHz IEEE 802.15. 4/ZigBee-ready RF Transceiver. *Available at <http://www.ti.com/lit/gpn/cc2420>* (2006), 53.
- [14] Alex King, James Brown, and Utz Roedig. 2014. DCCA: Differentiating Clear Channel Assessment for improved 802.11/802.15.4 coexistence. In *2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 45–50.

- [15] Chieh-Jan Mike Liang, Nissanka Bodhi Priyantha, Jie Liu, and Andreas Terzis. 2010. Surviving wi-fi interference in low power zigbee networks. In *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*. ACM, 309–322.
- [16] Shan Lin, Fei Miao, Jingbin Zhang, Gang Zhou, Lin Gu, Tian He, John A. Stankovic, Sang Son, and George J. Pappas. 2016. ATPC: Adaptive Transmission Power Control for Wireless Sensor Networks. *ACM Trans. Sen. Netw.* 12, 1, Article 6 (March 2016), 31 pages. <https://doi.org/10.1145/2746342>
- [17] Razvan Musaloiu-E and Andreas Terzis. 2008. Minimising the effect of WiFi interference in 802.15. 4 wireless sensor networks. *International Journal of Sensor Networks* 3, 1 (2008), 43–54.
- [18] Felix Jonathan Oppermann, Carlo Alberto Boano, Marco Antonio Zúñiga, and Kay Römer. 2015. Automatic Protocol Configuration for Dependable Internet of Things Applications. In *Proceedings of the 10th International Workshop on Practical Issues in Building Sensor Network Applications (SenseApp)*. IEEE, 742–750. <https://doi.org/10.1109/LCNW.2015.7365923>
- [19] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella. 2006. Performance study of IEEE 802.15.4 using measurements and simulations. In *IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006.*, Vol. 1. 487–492. <https://doi.org/10.1109/WCNC.2006.1683512>
- [20] Marina Petrova, Lili Wu, Petri Mahonen, and Janne Riihijarvi. 2007. Interference measurements on performance degradation between colocated ieee 802.11 g/n and ieee 802.15. 4 networks. In *Networking, 2007. ICN'07. Sixth International Conference on*. IEEE, 93–93.
- [21] Joseph Polastre, Jason Hill, and David Culler. 2004. Versatile Low Power Media Access for Wireless Sensor Networks. In *Proceedings of the 2Nd International Conference on Embedded Networked Sensor Systems (SenSys '04)*. ACM, New York, NY, USA, 95–107. <https://doi.org/10.1145/1031495.1031508>
- [22] Mo Sha, Gregory Hackmann, and Chenyang Lu. 2013. Energy-efficient low power listening for wireless sensor networks in noisy environments. In *Proceedings of the 12th international conference on Information processing in sensor networks*. ACM, 277–288.
- [23] Yong Tang, Zhipeng Wang, Tianyu Du, Dimitrios Makrakis, and Hussein T Mouftah. 2013. Study of clear channel assessment mechanism for ZigBee packet transmission under Wi-Fi interference. In *Consumer Communications and Networking Conference (CCNC), 2013 IEEE*. IEEE, 765–768.
- [24] Yong Tang, Zhipeng Wang, Dimitrios Makrakis, and Hussein T Mouftah. 2013. Interference Aware Adaptive Clear Channel Assessment for improving ZigBee packet transmission under Wi-Fi interference. In *2013 IEEE International Conference on Sensing, Communications and Networking (SECON)*. IEEE, 336–343.
- [25] Lieven Tytgat, Opher Yaron, Sofie Pollin, Ingrid Moerman, and Piet Demeester. 2012. Avoiding collisions between IEEE 802.11 and IEEE 802.15. 4 through coexistence aware clear channel assessment. *EURASIP Journal on Wireless Communications and Networking* 2012, 1 (2012), 1–15.
- [26] Ruitao Xu, Gaotao Shi, Jun Luo, Zenghua Zhao, and Yantai Shu. 2011. Muzi: Multi-channel zigbee networks for avoiding wifi interference. In *Internet of Things (iThings/CPSCoM), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*. IEEE, 323–329.
- [27] Sven Zacharias, Thomas Neue, Sinead O'Keefe, and Elfed Lewis. 2012. Identifying sources of interference in RSSI traces of a single IEEE 802.15. 4 channel. In *ICWMC 2012, The Eighth International Conference on Wireless and Mobile Communications*. 408–414.
- [28] Xiaolong Zheng, Zhichao Cao, Jiliang Wang, Yuan He, and Yunhao Liu. 2014. ZiSense: towards interference resilient duty cycling in wireless sensor networks. In *Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems*. ACM, 119–133.
- [29] Ruogu Zhou, Yongping Xiong, Guoliang Xing, Limin Sun, and Jian Ma. 2010. Zifi: wireless LAN discovery via ZigBee interference signatures. In *Proceedings of the sixteenth annual international conference on Mobile computing and networking*. ACM, 49–60.

Received October 2016; revised June 2017; accepted March 2018