LABeL: Link-based Adaptive BLacklisting Technique for 6TiSCH Wireless Industrial Networks

Vasileios Kotsiou, Georgios Papadopoulos, Periklis Chatzimisios, Fabrice Theoleyre

LABeL: Link-based Adaptive BLacklisting Technique for 6TiSCH Wireless Industrial Networks

Vasileios Kotsiou
ICube Lab, CNRS / University of Strasbourg
Illkirch, France
kotsiou@unistra.fr

Georgios Z. Papadopoulos
IMT Atlantique, IRISA, UBL
Rennes, France
georgios.papadopoulos@imt-atlantique.fr

Periklis Chatzimisios
CSSN Research Lab, Alexander TEI of Thessaloniki
Thessaloniki, Greece
peris@it.teithe.gr

Fabrice Théoleyre
ICube Lab, CNRS / University of Strasbourg
Illkirch, France
theoleyre@unistra.fr

ABSTRACT

Industrial applications require more and more low-power operations, low-delay, deterministic communications as well as end-to-end reliability close to 100%. However, traditional radio technologies are sensitive to external interference, which degrades the reliability and introduces unpredictable delays due to collision detection and retransmissions. Therefore, recent standardization efforts focus on slow channel hopping strategies to provide strict Quality of Service (QoS) for the Industrial Internet of Things (IIoT). By keeping nodes time-synchronized and by employing a channel hopping approach, IEEE 802.15.4-TSCH (Time-Slotted Channel Hoping) aims at providing high-level network reliability. However, some radio channels still suffer from high external interference and need to be *blacklisted*. Since the interference pattern is rather dynamic, unpredictable and highly localized, we here propose heuristics to decide which channels to blacklist. To avoid deafness, the transmitter and the receiver must also agree on a consistent blacklist. Furthermore, since the external interference may be time-dependent as well, we also propose mechanisms to decide when a channel has to be blacklisted or on the contrary recovered. Our thorough experimental evaluation based on OpenWSN and FIT IoT-LAB highlight the relevance of this approach: with a localized blacklisting strategy, we increase by 20% packet delivery rate for the worst links.

KEYWORDS

IoT; IEEE 802.15.4-2015; TSCH; Channel Hopping; Radio Characterization; Interference; Blacklisting; Experimental Evaluation;

1 INTRODUCTION

Wireless deployments are becoming broadly used and enable an Internet access for any user (and thing). Indeed, during the last years we have experienced the emergence of a new paradigm called Internet of Things (IoT) in which smart, uniquely identifiable and connected objects cooperatively construct a (wireless) network of things [2]. Those things can be deployed nearly everywhere, at homes, universities, cities, agricultural fields, even in human bodies.

Among the previously mentioned deployments, the Industry 4.0 is an emerging concept aiming at re-using the IoT automation to make the production chains more profitable by maximizing flexibility and adaptability in the factories. Industrial applications, such as vehicle automation, smart grid, automotive industry or airport logistics, share similar network performance requirements of including low-latency and high network reliability.

To provide Quality of Service (QoS) for industrial-like wireless networks, IEEE 802.15.4-2015 standard was published in 2016 [1]. Time-Slotted Channel Hoping (TSCH) is among the Medium Access Control (MAC) schemes defined in this standard. TSCH aims at low-power, deterministic and reliable wireless industrial networks. At its core, TSCH relies on scheduling by employing time synchronization to solve the contention in the wireless medium. To achieve low-power operations, a node turns its radio *ON* only when it transmits or receives a frame. Furthermore, TSCH supports a channel hopping approach to efficiently combat the noisy environments.

Number of research works related with radio characterization demonstrate that most of the IEEE 802.15.4 radio channels suffer from external interference in the 2.4 *GHz* band (e.g. [9, 14, 15, 25]). In particular, the IEEE 802.11 channels 1, 6 and 11 are extensively used and, thus, they interfere and heavily impact most of the IEEE 802.15.4 channels [11, 26]. As it is shown in Fig. 1, the 15, 20 and 25-26 IEEE 802.15.4 channels do not interfere with the popular IEEE 802.11 channels. In such harsh environments, channel hopping solutions are essential to combat external interference [26].

Since the overlapped channels may perform badly during long periods [11], the system should *blacklist* them in the channel hopping sequence. For instance, WirelessHART provides the possibility to *block* globally the bad channels [20] by removing them from the frequency hopping sequence for all the nodes. Blacklisting improves both reliability and energy efficiency, by reducing the amount of packet losses. However, we still have to propose localized strategies to detect and blacklist dynamically those bad channels.

In this paper, we focus on frequency hopping based approaches, and we aim at identifying the importance of implementing link-based blacklisting methods. We then propose LABeL, a Link-based Adaptive BLacklisting algorithm. To evaluate our mechanism, we

MSWiM '17, , November 21-25, 2017, Miami, FL, USA.

ACM ISBN ISBN 978-1-4503-5162-1/17/11…$15.00
https://doi.org/https://doi.org/10.1145/3127540.3127541

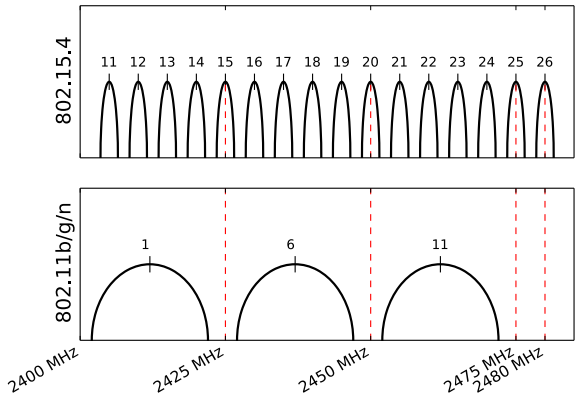


Figure 1: Overlapping IEEE 802.15.4 and IEEE 802.11 channels.

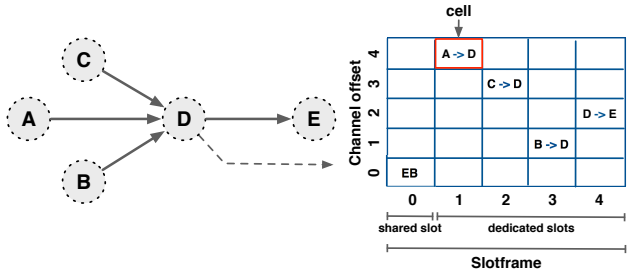


Figure 2: An example of TSCH scheduling for node D. A → D stands for *'A transmits to D'*, while Enhanced Beacon (EB) cells are used for broadcast and advertisement frames.

conduct a thorough experimental campaign, over the large Future Internet of the Things IoT-LAB platform based on M3 nodes and OpenWSN project that comes with a full 6TiSCH IoT stack, i.e., IEEE 802.15.4-TSCH, IPv6, 6TiSCH, Routing over Low Power and Lossy Networks (RPL), Constrained Application Protocol (CoAP). Our thorough experimental results highlight a significant increase of Packet Delivery Ratio (PDR), by 20% for the worst links.

The contributions of this paper are as follows:

(1) We provide an algorithm to determine dynamically which physical channels to blacklist. A set of *bad* channels is identified for each radio link. Since we do not exploit a *fixed* threshold value, we are able to identify bad channels even for weak links;
(2) We present a method to passively probe the bad channels, while limiting their impact on the energy consumption and the reliability;
(3) By exploiting 6P control packets, we detail techniques to maintain consistent blacklists for both the transmitter and the receiver and, thus, to avoid deafness [13];
(4) We propose a method to modify the frequency hopping sequence. This way, we make the collisions not repetitive, when two radio links use the same timeslot with a different channel offset and different blacklists;
(5) We experimentally validate our approach in the FIT IoT-LAB indoor testbed with the OpenWSN stack.

2 BACKGROUND & RELATED WORK

2.1 Channel Hopping-based Standards

Using a different physical channel for successive transmissions allows to reduce the impact of external interference and to improve the network reliability [26]. Indeed, the standardization bodies have proposed to use channel-hopping techniques, which allow subsequent packets to be transmitted over different frequencies, mainly to be utilized for industrial wireless networks. More specifically, the failed packet will be retransmitted through another physical channel, to increase the probability of successful reception, particularly in presence of narrow band external interference. Note that such protocols require strict guarantees in terms of time synchronization between the nodes within the wireless network [16].

IEEE 802.15.4-2015 has proposed the TSCH mode, largely inspired from the previous ISA100.11a [10] and WirelessHART [21] standards. In TSCH networks, time is divided into timeslots of equal length. At each timeslot, a node may transmit or receive a frame, or it may turn to sleep mode for saving energy. A set of timeslots constructs a slotframe. Each timeslot is labelled with an Absolute Sequence Number (ASN), a variable which counts the number of timeslots since the network was established. Based on the ASN and the schedule, the nodes in the TSCH network decide when to transmit or receive a frame.

IEEE 802.15.4-2015 TSCH implements a channel hopping approach to combat noise and interference and, thus, to achieve high network reliability [26]. To do so, TSCH presents a deterministic scheduling approach in which each cell consists of a pair of timeslot and channel offset for collision avoidance. The standard maintains a schedule, and assigns a set of cells to each radio link. At the beginning of each timeslot, the channel offset is translated into a physical channel using the ASN value:

$$frequency = F\Big(\big(ASN + channelOffset\big)\ \%\ nFreq\Big) \qquad (1)$$

where ASN denotes the Absolute Sequence Number of the timeslot, $channelOffset$ the channel offset of the current cell, and $nFreq$ is the number of available channels (e.g., 16 when using IEEE 802.15.4-compliant radios at 2.4 GHz with all channels in use) [27]. Finally, note that each cell can be either dedicated (contention-free) or shared (contention-based approach).

In Fig. 2, a TSCH schedule is illustrated. The Enhanced Beacons (EBs) are broadcast packets and use the first (shared) cell (with contention). All the other cells are dedicated, one transmission opportunity being here allocated per slotframe to each active radio link.

2.2 Blacklisting Techniques

Blacklisting consists in identifying the channels which exhibit the lowest reliability to avoid using them for the transmissions. Without channel hopping, it consists for each radio link in negotiating the most efficient channel to use for *all* its transmissions [22].

Channel hopping allows to minimize the impact of these *bad* channels [26]. However, they still negatively impact the number of (re)-transmissions and the reliability. Thus, blacklisting for slow frequency hopping consists in excluding the *bad* channels from the frequency hopping sequence. This technique has been used by several standards such as IEEE 802.15.4-2015 [1] and WirelessHART [20].

2.2.1 Detecting bad channels. Blacklisting a channel may also reduce the network capacity, since the same traffic has to be forwarded through a smaller number of channels. Thus, we have to carefully select the channels to blacklist, i.e., their usage has to significantly degrade the reliability.

Hanninen *et al.* [8] propose to blacklist a channel if the associated packets exhibit an average Received Signal Strength Indicator (RSSI) value below a given threshold. However, RSSI has been shown to inaccurately estimate link quality for both indoor [23] and outdoor [17] environments. Sha *et al.* [19] blacklist the channels when the link reliability is below a certain threshold and they also exploit the fact that adjacent channels often exhibit a similar behavior.

To recover, Tang *et al.* [22] remove a channel from the blacklist after a fixed period: the channel has to be probed again to be (re)-blacklisted. Thus, the blacklist is periodically flushed, and the node has to re-estimate the link quality, it keeps on continuously oscillating, needing time to re-blacklist a bad channel. We rather propose to adopt a *continuous* approach, *updating* the link quality of bad channels with a limited impact on data packet losses.

Chiti *et al.* [4] use a spectrum sensing technique during a few dedicated timeslots to identify which channels to blacklist. However, such method needs specific cells, during which no other node is allowed to transmit, thus, wasting bandwidth and energy.

2.2.2 Global vs. localized blacklisting. Bluetooth was also exploiting frequency hopping to improve the reliability. Zacharias *et al.* investigated the co-existence of Wi-Fi and Bluetooth networks [28], and proposed to blacklist the concerned WLAN channels for Bluetooth. However, only 1-hop topologies are considered.

In WirelessHART, the blacklisting solution is applied globally, where certain channels are blocked for the whole wireless industrial network [20]. Such approach may be suboptimal since a physical channel exhibits very location-dependent characteristics [11]. Even more, a *weak* radio link will be more impacted by external interference: the Signal-to-Noise-plus-Interference Ratio (SINR) margin is smaller. Thus, a per-link blacklist should be preferred to avoid wasting bandwidth.

In ISA100.11a [18], a localized blacklist may also be implemented. The node has the right to transmit during a cell if the channel offset does not give a blacklisted physical channel. Else, the node has to *skip* the cell until the channel offset gives an authorized physical channel. However, such approach has a very negative impact on the delay and the throughput: the transmitter has to defer its transmission until the frequency hopping sequence provides a non-blacklisted channel (in the next slotframe).

Du *et al.* [5] proposed a localized blacklisting method in TSCH, in which a pair of nodes negotiate the most accurate channels to use based on link quality indicators. To this aim, specific timeslots are reserved to measure the noise level on each physical channel. A node then exchanges with its neighbors its blacklist to agree on the channels to use. In this study, we do not dedicate additional resource to probe each channel. We also modify the pseudo-random sequence to avoid repetitive collisions when two interfering radio links do not use the same blacklist.

2.3 6TiSCH Overview

The 6TiSCH IETF working group aims to define a set of protocols to operate IPv6 (i.e., 6LoWPAN) over a reservation based MAC layer (i.e., TSCH). 6TiSCH defines the way to modify the schedule, using the protocol 6P. In a distributed scheme, the Scheduling Function (e.g., SF0 [6]) will decide how many cells to reserve with a neighbor. A 6P transaction then engages, transmitted through the shared cells, or specific dedicated cells if some are already present in the schedule. A two-way handshake is provided in 6P:

(1) The transmitter sends a 6P request in unicast, with a list of available cells. This request is acknowledged by the receiver;
(2) The receiver verifies a sufficient part of these cells are available in its schedule. It then constructs a 6P reply transmitted in unicast, acknowledged by the transmitter.

When the transaction has completed, both the transmitter and the receiver have modified consistently their schedule. In particular, the loss of acknowledgements is neglected: the 6P unicast packet has already reserved the medium and the level of external interference may be considered stable during a timeslot.

Alternatively, 6TiSCH also supports a global schedule computed by the Path Computation Element (PCE) and pushed to each node.

In this study, we design and develop LocAd, a localized and adaptive blacklisting scheme for TSCH. To this aim, we employ the OpenWSN, an implementation of a full protocol stack based on IoT standards (i.e., IEEE 802.15.4-TSCH, IPv6, 6TiSCH, RPL, CoAP).

3 PROBLEM STATEMENT & APPROACH

External interference may severely affect some IEEE 802.15.4 channels [26], requiring to blacklist the *bad* channels. However, the performance of a given physical channel depends heavily on the geographical location, and even on the link's characteristics [11].

We propose here to implement a *link-based* blacklisting algorithm, i.e., LABeL: the transmitter and the receiver have to agree on the blacklisted channels to not use for their transmissions. Different pairs of nodes would blacklist different channels resulting in increased frequency re-use. More specifically, each pair monitors the link quality across all the 16 available channels at 2.4 *GHz*, and decides which channels to utilize. Consequently, in this study, we focus on addressing the following challenges:

Overhead: We here implement a passive method to detect *bad* channels. No probing packets are required, increasing both the level of interference and the energy consumption. Instead, we use the data packets to continuously re-evaluate the quality of channels in order to appropriately insert or remove from the blacklist;

Time-variant: Under dynamic environments, the list of bad channels may change so frequently that blacklisting it would have no effect on the performance [11]. Control packets have to be exchanged to update the blacklist, which would annihilate the benefit of reducing the number of (re)transmissions to deliver a data packet to the next hop. We experimentally

verify that the PDR is actually improved with a localized adaptive blacklisting approach;

Inconsistency management: Two nodes agreeing on the list of bad channels, requires signaling (i.e., additional control packets). Since some control or acknowledgement packets may be lost, some inconsistencies may arise. As a result, they may operate with a different frequency hopping sequence, leading to potential deafness. We will propose robust mechanisms integrated to 6P in order to make the transactions reliable.

Minimization of collisions: When two interfering radio links use a different blacklist, they may collide even if they do not use the same channel offset, since Equation 1 depends on the blacklist's content (i.e., the number of available channels). We propose to modify the frequency hopping sequence to make the collisions less repetitive.

In this paper, we both propose the mechanisms to implement a link-based blacklist, and we evaluate thoroughly the blacklisting technique in a realistic testbed to demonstrate the advantages of such approach.

4 LOCALIZED AND PER-LINK ADAPTIVE BLACKLISTING UNDER IEEE 802.15.4-TSCH

A global blacklist exploits a list of *bad* channels that provide a low reliability due to the presence of interference. However, this list is location and time-dependent [11]: while a channel may perform badly for some radio links, it may provide a close to perfect reliability for some other radio links. Moreover, the same radio channel may perform well during the afternoon and night, however, its performance may drop during the day-time, due to the Wi-Fi activity.

The impact of external interference depends on the SINR margin of the radio link [7]. When the transmitter and the receiver are close to each other, the level of external interference has to be higher to impact the reliability. Thus, we here present an algorithm to incorporate a **localized** and **per-link** blacklist into IEEE 802.15.4-TSCH.

4.1 Deciding which channels to blacklist

In this study, we propose LABeL to identify the channels to blacklist, i.e., the set of channels that impact negatively the performance of the radio link and/or the network. According to our previous work, relying on RSSI or LQI metric is not representative of the channel quality [11]. Therefore, we focus on measuring the PDR performance, denoting accurately the ability of the link to deliver successfully the data packets.

To this aim, each node in a TSCH network computes the PDR of unicast data packets **independently** for each neighbor and channel. More precisely, a node counts the number of Acknowledgements (ACKs) and the number of packets transmitted to a particular neighbor N. Since we are interested in a per channel behavior, we compute this PDR value independently for each channel and neighbor:

$$PDR(N,c) = \frac{nb_{ack}(N,c)}{nb_{tx}(N,c)} \quad (2)$$

with $nb_{ack}[N,c]$ the number of ACKs received from N through the channel c, and $nb_{tx}[N,c]$ the number of packets transmitted to N.

We can note that a node that uses several tracks to the same neighbor may compute the average PDR for *all* the tracks. Indeed, external interference will impact equally each track, and we can aggregate the traffic of several tracks to more accurately identify the *bad* channels.

Most of the proposals use a fixed threshold value (e.g., [8], [19]): any radio channel that provides a PDR inferior to a pre-defined threshold value is blacklisted. However, the *average* PDR is very radio link-dependent: when the received signal strength is low, packets may be dropped even if no external interference is present. Low quality links are frequent in many deployments, while high quality links are often not sufficient to maintain a connected topology [12]. We have consequently focus on an **adaptive** approach in which this threshold depends on the link, and is not fixed a priori globally.

The Window Mean Exponential Weighted Moving Average estimator (WMEWMA) has been proved to accurately estimate the link quality [3]. Indeed, packet losses represent a stochastic variable and need to be *smoothen*. We consequently propose to use WMEWMA to independently measure the PDR for each channel. For this sake, a node counts the number of transmitted messages, and the number of acknowledgments received correctly. In this paper, each node computes the PDR for the last 16 transmitted packets for a given channel, and updates accordingly the smoothed PDR metric.

Algorithm 1 describes formally LABeL, our link-based and adaptive blacklisting approach. We first compute the average PDR of each channel independently, using the extended WMEWMA estimator (lines 3-4). Then, we identify the best channel, providing the highest PDR (lines 5-7), which allows us to define a dynamic PDR threshold value PDR_{th} to identify bad channels (lines 9-19). Note that we dynamically adapt PDR_{th} in order to maintain at minimum 3 whitelisted channels on each wireless link. Then, we update the blacklist. In particular, a given channel is considered as bad if it provides a PDR lower than PDR_{th} (lines 21-23). Inversely, a channel is removed from the blacklist if its PDR metric significantly exceeds the threshold value (lines 24-26).

Note that constructing a link-based blacklist requires only for the transmitter to collect the ratio of acknowledged packet. In particular, the blacklist considers both directions, for respectively the data frame and the acknowledgement transmissions. Thus, computing the blacklist does not need to send explicit control and probe packets, and does not generate any overhead. Note that the blacklist is updated continuously, i.e., at each data transmission, while 6P control packet is exchanged, only when the blacklist is modified.

4.2 Modifying the frequency hopping sequence

After identifying the blacklisted radio channels, we next have to exploit this blacklisting mechanism with TSCH. In particular, the employed physical channel is decided at the beginning of each cell, using Equation 1 (see Section 2.1).

Note that ISA100.11a [18] proposes to use a localized blacklist. A node follows the frequency hopping sequence. However, when the transmitter detects that the physical channel associated to a cell is blacklisted, it postpones its transmission (i.e., for the following

Algorithm 1: Blacklist construction

Data: $blacklist$ (current blacklist),
$nb_{tx}[CH]$ and $nb_{ack}[CH]$ (nb. of transmitted packets and received ACKs over each channel)
α (WMEWMA's parameter)
$\mathcal{T}$ (threshold to consider a channel bad)
Result: $blacklist$ (new list of bad channels)
// PDR for each channel
$best \leftarrow 0$;
for $c \in Channels$ **do**
  // WMEWMA of the PDR with the last 16 transmitted packets
  $PDR_{last16} \leftarrow \frac{nb_{ack}[c]}{nb_{tx}[c]}$;
  $PDR_{wmewma}[c] = \alpha PDR_{wmewma}[c] + (1-\alpha)PDR_{last16}$;
  // Remembers the PDR of the best channel
  if $best \leq PDR_{wmewma}[c]$ **then**
    $best \leftarrow PDR_{wmewma}[c]$;
  end
end
// Adaptive Threshold Calculation
repeat
  $numch \leftarrow 0$;
  $weight \leftarrow weight - 0.01$;
  $\mathcal{T} \leftarrow best * weight$;
  for $c \in Channels$ **do**
    if $PDR_{wmewma}[c] < \mathcal{T}$ **then**
      $numch \leftarrow numch + 1$;
    end
  end
until $numch \geq 3$;
// threshold PDR to define which channels perform significantly worse than the best one
$PDR_{th} \leftarrow \mathcal{T} * best$
// For each channel, verifies it performs similarly to the best one (or not)
for $c \in Channels$ **do**
  // To blacklist
  if $PDR_{wmewma}[c] < PDR_{th}$ **and** $c \notin blacklist$ **then**
    $blacklist \leftarrow blacklist + \{c\}$;
  end
  // To recover
  if $PDR_{wmewma}[c] > PDR_{th}$ **and** $c \in blacklist$ **then**
    $blacklist \leftarrow blacklist - \{c\}$;
  end
end
return blacklist;

slotframe, 101 timeslots in TSCH). Since the number of channels and the slotframe length are mutually prime numbers, the physical channel associated with the same cell in the next slotframe will be different. However, such technique presents two major drawbacks:

Delay: Since the transmission is postponed for the next slotframe, blacklisting would consequently increase the end-to-end delay. The jitter is also increased due to the fact that the delay increases if the channel offset leads to a blacklisted channel;

Bandwidth: Blacklisting a channel prevents to use the cell in all the corresponding slotframes. Thus, if X% of the channels are blacklisted, the radio link can only use (100-X%) of the radio bandwidth.

Let us assume that we adapt directly Eq. 1, where *nFreq* would be the number of non blacklisted channels, and $F()$ would map the values to the physical channels. Let us now consider two mutually interfering wireless links that use the same timeslot but a different channel offset. These links, would never collide, if they do not employ any blacklisting. However, if they use different blacklists, *different* channel offsets may map to the *same* physical channel.

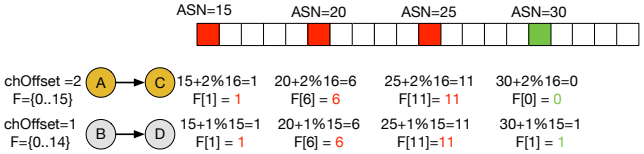


Figure 3: Colliding cells which use a different channel offset if we use the eq. 1 just changing the channel set — F[] denotes the set of *good* channels (the channel 15 is blacklisted for the link $B \rightarrow D$), the link $A \rightarrow C$ (resp. $B \rightarrow D$) is assigned the channel offset 2 (resp. 1).

Let's consider the scenario illustrated in Fig. 3. The pair A/C has no blacklisted channel, while B/D blacklisted the channel 15. Since the modulo changes, we may create several collisions in consecutive slotframes even when blacklisting only one channel.

Therefore, we propose to adapt the frequency hopping method, making the collisions non repetitive. We aim to minimize the number of collisions among interfering links that use a different channel offset if their blacklist differs slightly. To do so, we apply first the Equation 1 to compute the radio channel to use. Then, the algorithms makes the distinction between the following cases:

C1: **Good channel**: If the physical channel is not blacklisted, let's use it;

C2: **Blacklisted channel**: If the physical channel is blacklisted, let's select pseudo-randomly a good channel. The pseudo-random function must use a common knowledge between the receiver and the transmitter to avoid deafness. We propose to select the channel accordingly:

$$frequency = F\Big(\big(ASN + channelOffset + k\big) \ \% \ nFreq\Big) \qquad (3)$$

with k the minimum integer value such that 'frequency' corresponds to a *good* channel. Since ASN, $channelOffset$, $nFreq$ and the blacklist are common to the receiver and the transmitter, they will lead to a consistent decision.

Since we keep the same modulo operator, two cells with different channel offsets will never collide if the channel hopping sequence leads to a good channel. A collision may occur probabilistically if at least one of the radio links leads to a blacklisted channel during the corresponding slotframe. The probability of collision is then uniformly distributed among all the channels. In other words, such repartition may be considered like external interference and over-provisioned cells should be already reserved for retransmissions to cope with this situation.

4.3 Modifying the Channel Hopping Sequence to Passively Monitor the Quality of Bad Channels

We continuously estimate the PDR performance for all channels, including the blacklisted ones. Indeed, since the radio conditions may change during the deployment [11], we should recover a radio channel from a blacklist to whitelist, when its PDR performance exceeds

the threshold value (Algorithm 1, line 24). However, dedicating resource (control packets) to probe bad channels is not recommended since it would be costly in terms of energy consumption and additional unnecessary traffic. Note that is such case, the probe has to be done for each blacklisted channel for each radio link.

In this study, we rather propose to monitor the link quality using a passive method, exploiting directly the reliability statistics of data packets. However, a bad channel should be probed less frequently than a good channel since it has a negative impact on both the reliability and the energy consumption.

Therefore, we modify the previous second rule (C2) when computing the channel hopping sequence. More precisely, when Equation 1 returns a blacklisted channel:

C2.1: With the probability p, let's transmit the packet through this *bad* channel to keep on re-estimating the link quality for *all* channels;
C2.2: Otherwise, the transmitter and receiver select pseudo-randomly a good channel, applying the original C2 rule (cf. section 4.2).

A small p value means that the blacklisted channels will be probed infrequently. Re-estimating the quality consumes less resource, but requires a longer time to detect link quality change.

4.4 How to agree on a consistent blacklist in the transmitter and the receiver?

Recall, as previously detailed, each node calculates the number of ACKs received from a neighbor to compute the PDR. The transmitter then identifies the blacklisted channels according to their PDR by applying Algorithm 1. Hereafter, we should ensure that the transmitter and the receiver have the same blacklists, else they would use a different pseudo-random frequency hopping sequence, leading to a "deafness".

We focus here on providing a full blacklisting-enabled 6TiSCH stack. Thus, to this aim, the transmitter sends to the receiver its blacklist using a reliable method since the receiver is not aware of the actual statistics computed by the transmitter, and cannot construct the same blacklist. We here propose to exploit 6P to exchange the blacklists for each radio link (*e.g.*, *A*, *B*). More precisely, the transmitter *A* sends its blacklist in a 6P control packet. Note that 6P packets are transmitted through the shared cells and are prone to collisions: B needs to send an acknowledgement.

The IEEE 802.15.4 Information Elements (IEs) are a convenient option to include the backlist in the 6P packets. In our implementation, a node maintains for each of its active neighbors (i.e., to which it transmits packets) two blacklists:

(1) `tx-tmp`: the last backlist computed according to Algo. 1, not yet acknowledged by the receiver;
(2) `tx`: the last blacklist which was transmitted **and** acknowledged by the receiver.

Thus, we guarantee to use consistent blacklists for both sides. The list `tx-tmp` is used to construct a 6P IE. When the corresponding ACK is received, `tx-tmp` is copied in `tx` and then destroyed. Each node maintains different blacklists with each of its children. We thus achieve to define an adaptive, localized and per-link (per child) blacklisting algorithm.

Table 1: Experimental setup.

Topology	Parameter	Value
	Testbed site	Strasbourg site
	# of nodes	10
	# of Experiments	120
	Link Distance	$[2.0 - 14.3]$ *meters*
Experiment	**Parameter**	**Value**
	Duration	120 *min*
	Payload size	48 bytes
Protocol	**Parameter**	**Value**
CoAP	CBR (*Unicast*)	1 $pkts/3$ *sec*
RPL	DAO period	50 *s*
	DIO period	8.5 *s*
TSCH	Slotframe length	101
	NShared cells	5
	Timeslot duration	15 *ms*
	Maximum retries	3
Queues	Timeout	8 *s*
	Queue size	10 packets
	incl. data packets	Maximum 6 packets
Hardware	**Parameter**	**Value**
	Antenna model	Omnidirectional
	Radio propagation	2.4 *GHz*
	802.15.4 Channels	11 *to* 26
	Modulation model	AT86RF231 O-QPSK
	Transmission power	0 *dBm*

We assume that the loss of acks when the packet is received can be neglected. If the ack is lost, the blacklists may become inconsistent, and the transmitter at some time will try to update its blacklist.

5 EXPERIMENTAL PERFORMANCE EVALUATION

In this Section, we present a thorough experimental campaign over the FIT IoT-LAB platform[1] that is part of the FIT[2], an open large-scale and multiuser testing infrastructure for IoT-related systems and applications. Note that FIT IoT-LAB is a shared platform with potential concurrent experiments.

5.1 FIT IoT-LAB Platform

We conducted our study over the FIT IoT-Lab testbed, which belongs to the half real-world testbed category since several Wi-Fi Access Points (APs) are co-located. Thus, under such a realistic indoor environment, the nodes are subjected to external interference originated from Wi-Fi-based devices.

5.2 Experimental Setup and Parameters

In our experimental campaign, we employed M3 nodes, based on a STMicroelectronics 32-bit ARM Cortex-M3 micro-controller (ST2M32F103REY) that embeds an AT86RF231 radio chip, providing an IEEE 802.15.4 compliant PHY layer.

[1] https://www.iot-lab.info/
[2] https://fit-equipex.fr/

We focused on a 1-hop scenario with 10 M3 nodes to focus on the performance of a given radio link. We performed 120 experiments, while each experiment lasted for 120 *min*. The transmitter (leaf) node implements a Constant Bit Rate (CBR) application model, by transmitting 1 data packet every 3 *seconds*, at 0 *dBm* transmission power, resulting in more than 2000 *pkts* transmissions in total per experiment. We chose a 48 *bytes* data size, which corresponds to the general information used by monitoring applications (e.g., node ID, packet sequence, sensed value). The details of the setup are exposed in Table 1. We systematically plotted the 95% confidence intervals (each radio link denoting a dataset).

To conduct our experiments, we employed OpenWSN[3], an open-source implementation of a full protocol stack based on loT standards (IEEE 802.15.4-TSCH, IPv6, 6TiSCH, RPL, CoAP). In particular, we used the modified implementation of OpenWSN [4] for distributed scheduling with traffic isolation [24], to reserve a set of cells *per* flow.

5.3 Blacklisting Methods to Compare

We compared the following blacklisting methods:

- **Default:** TSCH network operates in standard mode and uses only channel hopping to defeat external interference;
- **Global Blacklisting**: We blacklist statically the three channels which are the most impacted by the interfering Wi-Fi networks — channel 12, 13 and 14;
- **Local-Fixed**: We blacklist all channels that exhibit a PDR lower than a fixed threshold value. This blacklist is then used in LocAd to modify the pseudo-random channel hopping sequence. Note that if all 16 radio channels present a performance lower that the pre-defined threshold, we select the channel with the best PDR value.
- **Local-Adaptive: LABeL**: The blacklist is computed based on Algo. 1. It is established as a per link basis, selecting the channels which perform significantly worse than the best ones. Thus, a channel is blacklisted not anymore only because it performs poorly, but more importantly if it exhibits a PDR significantly lower than the best channels for the *same* link. In other words, we avoid penalizing the links with a mediocre quality.

5.4 Studied Metrics

We measured the following metrics to evaluate the network performance:

- **Packet Delivery Ratio (PDR):** The ratio of the number of frames correctly acknowledged by the receiver and the number of frames transmitted by the transmitter. The PDR is measured at the MAC layer: one packet with one retransmission results a PDR of 50%;
- **Delay:** The average time between the generation of a packet and the reception of the corresponding acknowledgement. This average delay is computed only for the packets successfully delivered to the receiver;
- **Jitter:** The average difference for a given flow between its actual end to end delay and its average value;
- **Blacklist size:** The number of channels present in the blacklist;
- **ETX:** The average number of transmissions and retransmissions for each data frame. This metric is relative to the energy consumption: more cells and transmissions are required to deliver each data packet.

[3] http://www.openwsn.com

[4] branch *"track"* of https://github.com/ftheoleyre/openwsn-fw/ and https://github.com/ftheoleyre/openwsn-sw/

6 PERFORMANCE EVALUATION

6.1 Reliability

We first focus on the reliability performance and measure the PDR provided by a given link (Fig. 4a). To investigate the impact of the signal strength by grouping together the links with approximatively the same geographical length (in our testbed, the signal strength and the geographical length are quite strongly correlated variables).

For short (and strong) links, PDR is very high (≈100%) whatever the employed blacklisting technique (Fig. 4a). However, blacklisting technique improves slightly the PDR, even for strong links.

Weaker links tend to be more sensitive to external interference since their SINR margin is smaller. The *bad* channels, with a large level of external interference, impact negatively the reliability. All the blacklisting techniques improve in some extent the PDR. The global blacklisting provides the lowest improvement: some channels perform *badly* only for *some* radio links while they are blacklisted globally. Local blacklisting with a fixed threshold value is also suboptimal: a weak radio link tends to exhibit a low average PDR for all its channels. Thus, a medium PDR does not mean that a channel should be blacklisted. LABeL, computing dynamically the threshold value for the PDR, according to the best channels, is more effective to blacklist only the less efficient channels.

Next, we measured the Expected Transmission Count (ETX) in Fig. 4b. ETX is related to the energy efficiency since a node has less packets to transmit on average to deliver correctly a data packet. As can be observed, LABeL, the link-based adaptive scheme, provides an ETX below 1.1, making on average links more robust (14% less transmissions compared to without backlisting).

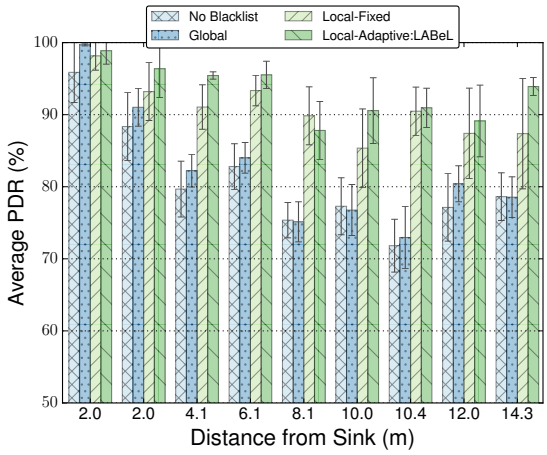
6.2 Blacklist size

We measured the average number of channels present in the blacklist (Fig. 5). The global blacklist is not represented since we fixed statistically its composition, including the three channels most impacted by Wi-Fi.

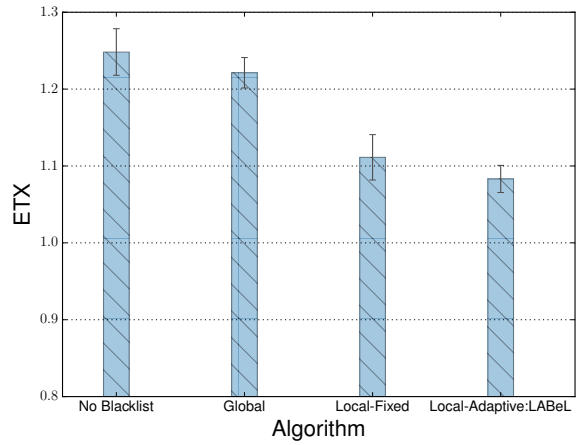
Our results demonstrate that the stronger the links, the fewer the blacklisted channels. Besides, we can verify that using a fixed threshold is suboptimal and aggressive: it tends to blacklist also channels which are close to the best ones, but below the fixed threshold. It is straightforward that using weaker links means also blacklisting more channels, whatever the blacklisting method is.

6.3 Delay

We finally consider the delay (in number of timeslots) between the packet's generation and the reception of the acknowledgement from the receiver (Fig. 6a). The global backlisting technique does not succeed to blacklist the worst channels: some keep on providing a low reliability and the packet has to be retransmitted. Indeed, it increases the average delay, while the standard deviation is much larger: some radio links are very negatively impacted by the non-blacklisted bad channels. On the contrary, local blacklisting allows



(a) Packet Delivery Ratio.



(b) Average number of transmissions before receiving an ack.

Figure 4: Per link reliability achieved with the different blacklisting methods.

to block the usage of the worst channels and to reduce the amount of retransmissions, thus, it reduces the delay.

In the Industrial Internet of Things (IIoT), a deterministic and predictable performance is required. Therefore, we focus specifically in Fig. 6b on jitter. While the non-blacklisting technique provides the highest jitter due to retransmissions, LABeL successfully identifies and exploits only the best channels and provides decreased jitter values.

7 CONCLUSIONS & FUTURE WORK

Recent standardization efforts such as WirelessHART, ISA100.11a and IEEE 802.15.4, focus on channel hopping strategies to improve the performance of industrial networks. Thus, we need algorithms able to *blacklist* a set of *bad* channels to use only the most reliable one. Since we face a very location and link-dependent performance, we here propose LABeL, a localized and link-based adaptive

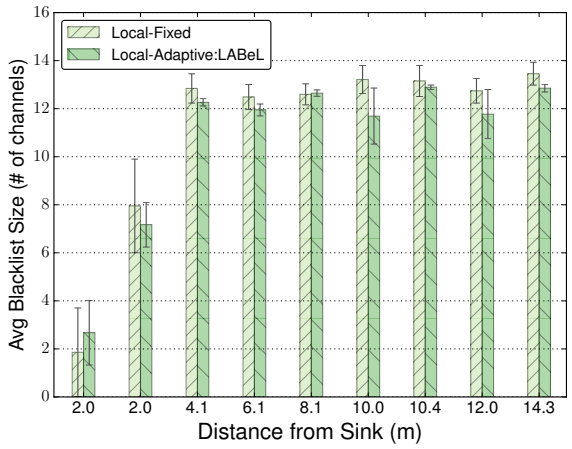


Figure 5: Average number of channels present in the blacklist.

blacklisting technique. By employing the WMEWMA estimator paired with a dynamic PDR threshold, we identify the bad channels. We also modify the pseudo-random channel hopping sequence to keep on probing the *bad* channels to recover, while minimizing the amount of bandwidth and energy required for measurement. Furthermore, we propose to modify the translation of a channel offset in a physical frequency to minimize the amount of collisions among interfering radio links and making them less repetitive. Our thorough experimental evaluation based on OpenWSN (implementation of 6TiSCH stack) and FIT IoT-LAB platform, exhibits that LABeL, an adaptive and link-based blacklisting technique, improves the reliability performance (by 20%) as well as it reduces the unnecessary traffic in the network while improving the jitter performance.

In the future, we plan to extend our experimental evaluation by also considering outdoor testbeds as well as other channel hopping protocols. Identifying the bad channels represents a challenging task. For instance, blacklisting the channels providing a bad PDR may lead to a bias if only a few packets are forwarded through a given link. Thus, it would be interesting to study methods that do not rely directly on the PDR.

REFERENCES

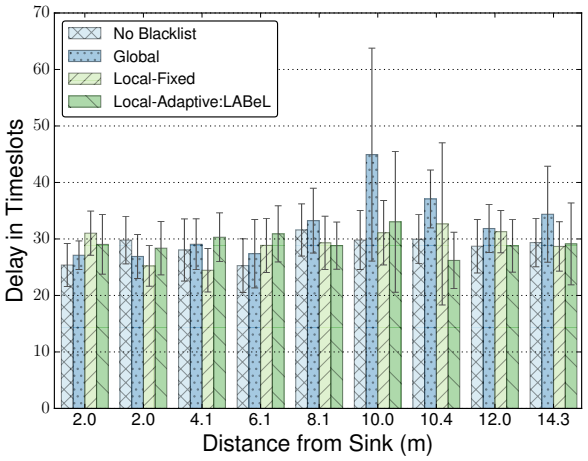
[1] 2016. IEEE Standard for Low-Rate Wireless Personal Area Networks (LR-WPANs). *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)* (April 2016). https://doi.org/10.1109/IEEESTD.2016.7460875

[2] Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2010. The internet of things: A survey. *Computer networks* 54, 15 (2010), 2787–2805.

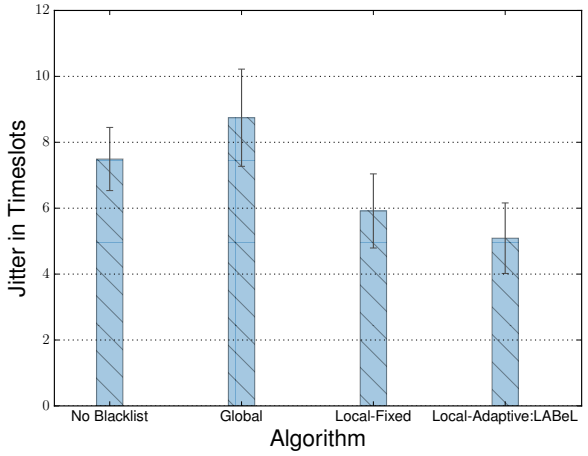
[3] Nouha Baccour, Anis Koubâa, Luca Mottola, Marco Antonio Zúñiga, Habib Youssef, Carlo Alberto Boano, and Mário Alves. 2012. Radio Link Quality Estimation in Wireless Sensor Networks: A Survey. *ACM Trans. Sen. Netw.* 8, 4, Article 34 (Sept. 2012), 33 pages. https://doi.org/10.1145/2240116.2240123

[4] F. Chiti, R. Fantacci, and A. Tani. 2017. Performance Evaluation of An Adaptive Channel Allocation Technique for Cognitive Wireless Sensor Networks. *IEEE Transactions on Vehicular Technology* 66, 6 (June 2017), 5351 – 5363. https://doi.org/10.1109/TVT.2016.2621140

[5] P. Du and G. Roussos. 2012. Adaptive time slotted channel hopping for wireless sensor networks. In *CEEC*. IEEE. https://doi.org/10.1109/CEEC.2012.6375374



(a) Delay (in timeslots).



(b) Jitter (in timeslots).

Figure 6: Time required for a given link to receive an ack for a transmitted packet.

[6] D. Dujovne, LA. Grieco, MR. Palattella, and N. Accettura. 2016. *6TiSCH 6top Scheduling Function Zero (SF0).* draft 2. IETF.

[7] Andrea Goldsmith. 2005. *Wireless Communications.* Cambridge University Press.

[8] Markku Hänninen, Jukka Suhonen, Timo D Hämäläinen, and Marko Hännikäinen. 2011. Link Quality-Based Channel Selection for Resource Constrained WSNs. In *GPC*. Springer.

[9] Anwar Hithnawi, Hossein Shafagh, and Simon Duquennoy. 2014. Understanding the Impact of Cross Technology Interference on IEEE 802.15.4. In *International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WiNTECH)*. ACM, 49–56. https://doi.org/10.1145/2643230.2643235

[10] ISA-100.11a-2011:. May 2011. Wireless Systems for Industrial Automation:Process Control and Related Applications. *International Society of Automation (ISA) Std.* 1 (May 2011).

[11] V. Kotsiou, G. Z. Papadopoulos, P. Chatzimisios, and F. Theoleyre. 2017. Is Local Blacklisting Relevant in Slow Channel Hopping Low-Power Wireless Networks?. In *Proceedings of the IEEE International Conference on Communications (ICC)*.

[12] Y. Liu, Y. He, M. Li, J. Wang, K. Liu, and X. Li. 2013. Does Wireless Sensor Network Scale? A Measurement Study on GreenOrbs. *IEEE Transactions on Parallel and Distributed Systems* 24, 10 (Oct 2013), 1983–1993. https://doi.org/10.1109/TPDS.2012.216

[13] G. Z. Papadopoulos, J. Beaudaux, A. Gallais, P. Chatzimisios, and T. Noel. 2014. Toward a Packet Duplication Control for Opportunistic Routing in WSNs. In *Proc. of the IEEE Global Communications Conference (GLOBECOM)*. 94–99.

[14] G. Z. Papadopoulos, A. Gallais, G. Schreiner, E. Jou, and T. Noel. 2017. Thorough IoT testbed Characterization: from Proof-of-concept to Repeatable Experimentations. *Elsevier Computer Networks* 119 (2017), 86–101.

[15] G. Z. Papadopoulos, A. Gallais, G. Schreiner, and T. Noel. 2016. Importance of Repeatable Setups for Reproducible Experimental Results in IoT. In *PE-WASUN*. ACM.

[16] G. Z. Papadopoulos, A. Mavromatis, X. Fafoutis, N. Montavont, R. Piechocki, T. Tryfonas, and G. Oikonomou. 2016. Guard Time Optimisation and Adaptation for Energy Efficient Multi-hop TSCH Networks. In *WF-IoT*. IEEE.

[17] Bogdan Pavkovic, Fabrice Theoleyre, Dominique Barthel, and Andrzej Duda. 2010. Experimental Analysis and Characterization of a Wireless Sensor Network Environment. In *PE-WASUN*. ACM.

[18] S. Petersen and S. Carlsen. 2011. WirelessHART Versus ISA100.11a: The Format War Hits the Factory Floor. *IEEE Industrial Electronics Magazine* 5, 4 (Dec 2011), 23–34. https://doi.org/10.1109/MIE.2011.943023

[19] M. Sha, G. Hackmann, and C. Lu. 2011. ARCH: Practical Channel Hopping for Reliable Home-Area Sensor Networks. In *RTAS*. IEEE. https://doi.org/10.1109/RTAS.2011.36

[20] Jianping Song, Song Han, A.K. Mok, Deji Chen, M. Lucas, and M. Nixon. 2008. WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control. In *RTAS*. IEEE.

[21] WirelessHART Specification. 2008. 75: TDMA Data-Link Layer. *HART Communication Foundation Std., Rev* 1 (2008).

[22] Lei Tang, Yanjun Sun, Omer Gurewitz, and David B. Johnson. 2011. EM-MAC: A Dynamic Multichannel Energy-efficient MAC Protocol for Wireless Sensor Networks. In *Proceedings of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '11)*. ACM, New York, NY, USA, Article 23, 11 pages. https://doi.org/10.1145/2107502.2107533

[23] L. Tang, K. C. Wang, Y. Huang, and F. Gu. 2007. Channel Characterization and Link Quality Assessment of IEEE 802.15.4-Compliant Radio for Factory Environments. *IEEE Transactions on Industrial Informatics* 3, 2 (May 2007), 99–110. https://doi.org/10.1109/TII.2007.898414

[24] F. Theoleyre and G. Papadopoulos. 2016. Experimental Validation of a Distributed Self-Configured 6TiSCH with Traffic Isolation in Low Power Lossy Networks . In *MSWiM*. ACM.

[25] L. Tytgat, O. Yaron, S. Pollin, I. Moerman, and P. Demeester. 2015. Analysis and Experimental Verification of Frequency-Based Interference Avoidance Mechanisms in IEEE 802.15.4. *IEEE/ACM Transactions on Networking* 23, 2 (April 2015), 369–382. https://doi.org/10.1109/TNET.2014.2300114

[26] Thomas Watteyne, Ankur Mehta, and Kris Pister. 2009. Reliability Through Frequency Diversity: Why Channel Hopping Makes Sense. In *PE-WASUN*. ACM.

[27] T. Watteyne, M. Palattella, and L. Grieco. 2015. Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement. RFC 7554. (2015).

[28] S. Zacharias, T. Newe, S. O'Keeffe, and E. Lewis. 2012. Coexistence measurements and analysis of IEEE 802.15.4 with Wi-Fi and bluetooth for vehicle networks. In *International Conference on ITS Telecommunications*. IEEE, 785–790. https://doi.org/10.1109/ITST.2012.6425289