Is Local Blacklisting Relevant in Slow Channel Hopping Low-Power Wireless Networks?

Vasileios Kotsiou, Georgios Papadopoulos, Periklis Chatzimisios, Fabrice Theoleyre

Is Local Blacklisting Relevant in Slow Channel Hopping Low-Power Wireless Networks?

Vasileios Kotsiou*, Georgios Z. Papadopoulos†, Periklis Chatzimisios‡ and Fabrice Tholeyre*

*ICube Laboratory, University of Strasbourg, France {*kotsiou, theoleyre*}@unistra.fr
†IRISA, Télécom Bretagne, Institut Mines-Télécom, France *georgios.papadopoulos*@telecom-bretagne.eu
‡CSSN Research Lab, Department of Informatics, Alexander TEI of Thessaloniki, Greece *peris*@it.teithe.gr

***Abstract*—With the large growth of the Internet of Things (IoT), a strong focus has been put on designing and developing energy efficient and high performance protocols. Industrial-type wireless networks require strict and on-time delivery guarantees, such as close to 100% network reliability and ultra low delay. To this aim, standards such as IEEE 802.15.4-TSCH or Wireless HART, aim to guarantee high-level network reliability by keeping nodes time-synchronized and by employing a slow channel hopping pattern to combat noisy environments and external interference. In wireless networks, since all the radio channels are not impacted in a similar manner, blacklisting bad channels may improve performance of the whole wireless infrastructure. In this paper, we perform a thorough experimental study to characterize the radio (for all IEEE 802.15.4 channels) and connectivity among the nodes of an indoor testbed. More precisely, we investigate the locality of these blacklisting techniques and we highlighted: the fact that some channels perform poorly only in a small set of locations, for certain radio links. Our study tends to justify the need for local blacklisting techniques, demanding more control packets, but dealing more efficiently with spectral re-use.**

***Index Terms*—IoT; IEEE 802.15.4; TSCH; Channel Hopping; Radio Characterization; Interference; Blacklisting; Experimental Evaluation;**

I. Introduction

Wireless industrial applications, such as e-health, cargo transportation, smart buildings, automotive industry or airport logistics, all share the aspect of including very low latency and high network reliability. However, most of the previously mentioned industrial networks cannot accommodate a best effort approach. These strict guarantees and requirements lead researchers to design deterministic algorithms for medium access [1]. Therefore, the current standards and technologies must consider the best effort traffic within the functionality of the wireless infrastructure in order to provide stable and predictable performance.

IEEE 802.15.4-2015 standard was published in 2016 [2] to provide certain quality of service for deterministic industrial-like wireless networks. Among the Medium Access Control (MAC) schemes defined in this standard, Time-Slotted Channel Hopping (TSCH) targets at realizing lower-power, low-delay and reliable networking solutions [3]. At its core, TSCH is a deterministic protocol and, thus, it relies on scheduling by employing time synchronization to solve the contention for medium access and to achieve a low-power operation. Thus, a node turns its radio ON only when it transmits or receives a frame.

TSCH employs a channel hopping approach to efficiently combat interference. Indeed, since external interference affects only certain IEEE 802.15.4 radio channels [4], the loss probability of one packet and its retransmissions are not anymore correlated. As a result, the *black period* during which no packet can be received correctly is shortened, leading to a more robust protocol. Furthermore, channel hopping solutions often support blacklisting techniques to block bad channels (i.e., low reliability, high variations). For instance, in Wireless HART, a list of bad channels is distributed to the nodes to forbid these channels in their channel hopping sequence [5].

In this paper, we conduct a thorough experimental study, over the FIT IoT-LAB platform, to characterize the IEEE 802.15.4 radio channels. In particular, we aim at verifying the importance and relevance of implementing local blacklisting methods, which require more signaling to maintain consistent schedules. In this study, we aim at filling the existing gap, to give arguments and justifications to spend effort and energy to implement a local blacklisting method.

The contributions of our work are as follows:

1) We first experimentally study a TSCH network by employing the OpenWSN stack to characterize the radio link quality in an indoor environment, i.e., FIT IoT-LAB;
2) We then analyze the time variability of the characteristics of the radio link quality, and particularly the dependency on the physical channel;
3) We finally investigate the geographical dependency of the bad radio channel list.

II. Background & Related Work

A. Experimental Characterization

In the research community, many studies have been conducted to characterize wireless communications. We here present the key characteristics of a multihop wireless environment.

Cerpa *et al.* [6] experimentally demonstrated that certain radio links in a testbed may be asymmetrical, while the radio link quality may not be perfectly correlated with its euclidean distance. The same authors have also highlighted the high variability of the quality of some radio links [7].

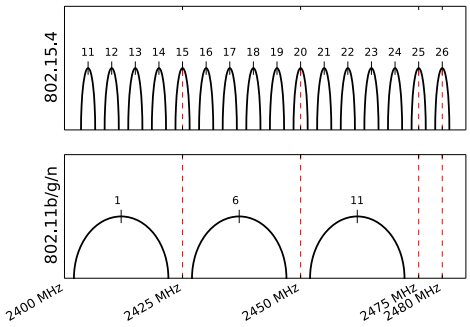


Fig. 1: Overlapping IEEE 802.15.4 & IEEE 802.11 channels.

Papadopoulos *et al.* [4], [8] experimentally investigated the time-dependency of the radio link quality. To do so, they repeated the experiments seven times over different days and time periods of each day. The authors identified that only very few links (i.e., less than 10%) remain stable and good in time.

Watteyne *et al.* [9] conducted an experiment study to record the connectivity between 350 nodes in a typical office environment. In particular, the authors exhibited the impact of WiFi interference on the reliability of the IEEE 802.15.4 channels. Moreover, the experimental results demonstrate that the quality of each link depends on the communication channel.

B. Channel Hopping MAC

In this paper, we focus on channel hopping approaches, a technique that allows for transmitting subsequent packets over different channels. If a failed packet is retransmitted through another physical channel, the protocol increases the success probability, particularly in presence of narrow band external interference.

In particular, for WiFi-enabled devices the IEEE 802.11 channels 1, 6 and 11 are extensively used and, thus, they interfere and negatively impact most of the IEEE 802.15.4 channels. As it is shown in Fig. 1, only the 11, 14-16, 19-21 and 24-26 IEEE 802.15.4 channels tend to perform well when the network is colocated with IEEE 802.11. In such harsh scenarios, channel hopping solutions are particularly efficient to combat external interference [10].

1) WirelessHART: The standard employs a central network manager to schedule communication among the devices, while it replaces Carrier Sense Multiple Access (CSMA) in the IEEE 802.15.4 with multi-channel Time Division Multiple Access (TDMA). Furthermore, WirelessHART uses a channel hopping approach across the 15 available frequency channels in the $2.4\ GHz$ band [11].

2) ISA100.11a: The standard aims to guarantee a deterministic communication latency, while increasing network reliability [12]. It combines CSMA-CA and slow channel hopping, excluding the overlap with the IEEE 802.11 channels. Furthermore, its hopping pattern separates the radio channels by at least three IEEE 802.15.4 channels (i.e., $15\ MHz$).

3) IEEE 802.15.4-2015-TSCH: The standard maintains a schedule, and assigns a collection of timeslots as well as *channel offsets* to each radio link. At the beginning of each timeslot, the channel offset is translated to a physical channel using the ASN (Absolute Sequence Number), a variable that counts the number of timeslots since the network was established.

C. Blacklisting bad channels

As previously discussed, external interference may severely affect IEEE 802.15.4 channels. However, we must note that not all radio channels experience the same level of interference. Thus, as discussed in [10] in order to mitigate such inefficiency, the incriminated channels may be *blacklisted*. This concept allows TSCH-like protocols to operate only over high quality radio channels, blocking from use the heavily interfered channels. Thus, a channel hopping approach actually employ the removal of the blacklisted channels from the hopping sequence. This technique has been utilized by a number of standardization bodies [2], [5].

In WirelessHART, the blacklisting solution is applied globally for the whole network [5]. In ISA100.11a [13], a local 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. Since the node has to *skip* the blacklisted cell until the channel offset leads to an authorized physical channel, delay and throughput are both impacted. Hanninen *et al.* [14] propose to measure the Received Signal Strength Indication (RSSI) periodically with each neighbor. However, the RSSI has been proved to inaccurately estimate link quality [15]. Sha *et al.* [16] blacklist the channels when the link reliability that is estimated via the Expected Transmission Count (ETX) is below a certain threshold. The authors also exploit the fact that adjacent channels often exhibit a similar behavior. Du *et al.* [17] propose a localized blacklisting method for TSCH in which specific timeslots are reserved to measure the noise level on each physical channel. A node then exchanges with its neighbors its blacklist in order to finally agree which channels will utilize.

III. Global vs. Local Blacklisting

The blacklisting technique combats external interference impacting only a subset of the IEEE 802.15.4 channels. In particular, by avoiding the blacklisted channels, we decrease the number of retransmissions and, thus, we improve both energy efficiency and delay.

However, blacklisting a channel globally might be suboptimal, since certain radio links may perform well for this channel. Moreover, with a centralized Path Computation Element (PCE), the scheduler has to allocate the same traffic to a smaller number of available channels and, thus, the network capacity decreases. In a similar manner, a distributed scheduling would lead to an increasing number of collisions and, thus, less frequency re-use.

On the other hand, local blacklisting techniques employ an adaptive approach. More specifically, each pair of nodes monitors its link quality and decides which channels to use for its transmissions. Different pairs would blacklist different channels resulting in increased frequency re-use. However, different local blacklists for different radio links present the following cost:

Overhead: Agreeing on the list of bad channels requires signaling. Each side of the radio link has to estimate the link quality and then to exchange its respective blacklisted channels, so that the union of the *bad* channels are blacklisted;

Time-variant: If the list of bad channels changes very frequently (e.g., every 10 sec), then local blacklisting is useless. Indeed, more signaling packets have to be transmitted in order to update the blacklist than the actual amount of retransmitted packets due to *bad* channels;

Inconsistency management: After the execution of a distributed algorithm, we may face certain inconsistencies. In particular, the transmitter may not have exactly the same blacklist as the receiver, because e.g., the last advertisement was not received. In this case, the pseudo-random hopping sequence is different, leading to packet losses. A recovery procedure has to be implemented, which may impact delay and reliability in a negative manner.

In this study, we perform an experimental characterization of the radio environment to verify and demonstrate that local blacklisting techniques are essential approaches in wireless communications and in particular for IoT, since the radio links present a different behaviors based on their operation area.

IV. Experimental Study

In this Section, we present a thorough experimental study 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.

A. FIT IoT-LAB Platform: Grenoble's site

In this investigation, our study was conducted over the testbed located in Grenoble (cf. Fig. 2). This testbed belongs to the real-world testbed category, since several WiFi Access Points (APs) are deployed in the building. Under such a realistic indoor environment i.e., a typical office space, the nodes are subjected to external interference originated from wireless devices using other technologies, such as Wi-Fi (in the 2.4 GHz band).

As depicted in Fig. 2, this testbed consists of 380 nodes deployed in an area of 65 m × 30 m. Most of the deployed sensor nodes (i.e., 90%) are placed under the raised floor, while the remaining 10% are deployed above the dropped ceiling.

B. Experimental Setup and Parameters

In our experimental study, 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.

We focused on a scenario with two M3 nodes, a transmitter and a receiver, respectively, positioned in a distance that varies from 0.6 to 17 m. In particular, at each experimental round, we selected randomly two different M3 nodes (out of 380) in the testbed to achieve maximum pluralism and transparency in our performance evaluation. Other nodes may be reserved for concurrent experiments by other researchers, and may generate external interference. We implement a Constant Bit Rate (CBR) traffic (20 packets / min), at 0 dBm transmission power, resulting in more than 1800 $pkts$ transmissions in total. We utilize a 48 $bytes$ data size, which corresponds to the general information used by monitoring applications (e.g., node ID, packet sequence, sensed value). We use the default TSCH and 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e) configurations as depicted in Table I. We performed a thorough analysis of the radio links by iterating the previously presented set of experiments over all IEEE 802.15.4 channels from 11 to 26. Finally, we ran more than 200 experiments, while each experiment lasted for 90 min. The details of the setup are exposed in Table I.

To conduct our experiments, we employed OpenWSN[3], an open-source implementation of a full protocol stack based on IoT standards (IPv6, 6TiSCH, RPL, CoAP). In particular, we used the modified implementation of OpenWSN[4] to handle tracks and to provide distributed scheduling [18].

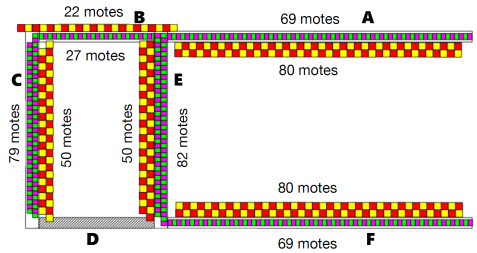


Fig. 2: Grenoble FIT IoT-LAB testbed map.

TABLE I: Experimental setup.

Topology	Parameter	Value
	Testbed organization	Grenoble site
	Number of nodes	2
	Number of Experiments	200
	Link Distance	$[0.6 - 17]$ $meters$
Experiment	**Parameter**	**Value**
	Duration	90 min
	Payload size	48 bytes
Protocol Stack	**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

[1]https://www.iot-lab.info/

[2]https://fit-equipex.fr/

[3]https://openwsn.atlassian.net/

[4]https://github.com/ftheoleyre/openwsn-fw/, and https://github.com/ftheoleyre/openwsn-sw/

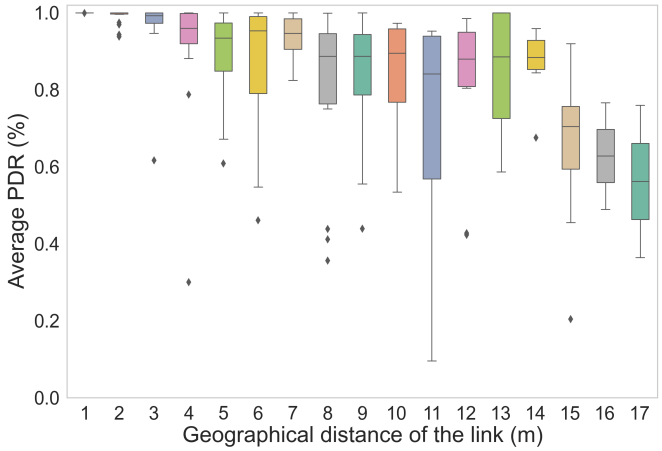


Fig. 3: PDR versus distance from the source.

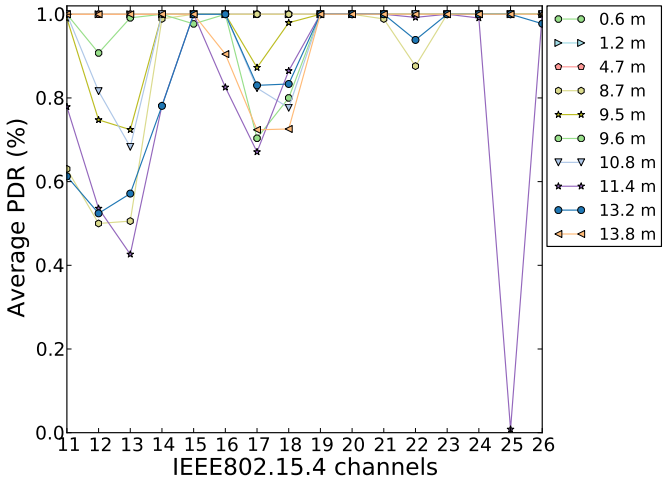


Fig. 4: PDR through all IEEE 8021.5.4 channels and over various distances (i.e., $0.6 - 13.8\ m$).

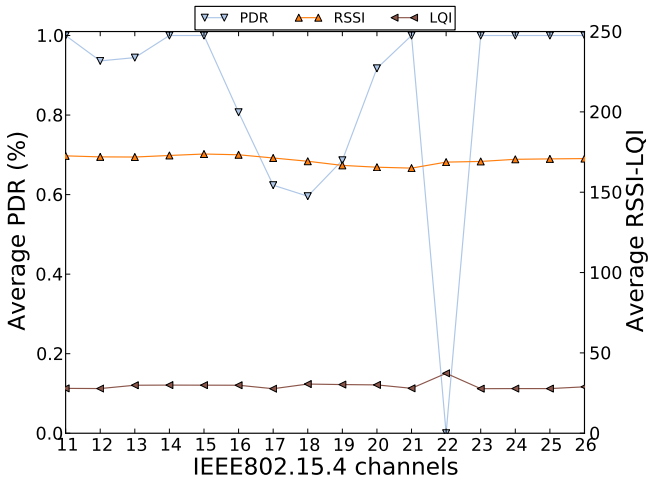


Fig. 5: Link Quality Indicators for the link with distance of $13.2\ m$.

In this study, we kept our experimental setup as simple as possible, in order to focus on the actual performance of the open testbed. Hereafter, we detail the results obtained from our experimentations, in terms of radio link quality characterization, stability of the radio links in time as well as channel characterization.

V. Radio Link Quality Characterization

In this Section, we investigate the impact of bad channels, due to external interference, on the performance of the system when a channel hopping approach is implemented.

A. Radio Link Reliability

We first measured the Packet Delivery Ratio (PDR) for all pairs of nodes that were randomly selected. We then grouped the pairs that provide approximatively the same geographical distance, (i.e., more or less $1\ meter$). As it can be observed from Fig. 3, short distance radio links ($< 3\ meters$) present very high link quality performance (i.e., close to 100%). Because the transmission power remains constant and the signal strength is high and, thus, limiting the number of errors of transmission. As a result, no blacklisting technique is required for such links.

On the contrary, the longer distance radio links present a very dynamic behavior. In particular, we can observe a straightforward relation between distance and link quality; if the distance between two nodes is longer, their PDR performance significantly drops, while the link quality discrepancy considerably increases. Thus, due to this strong variability, the long distance links need further investigation.

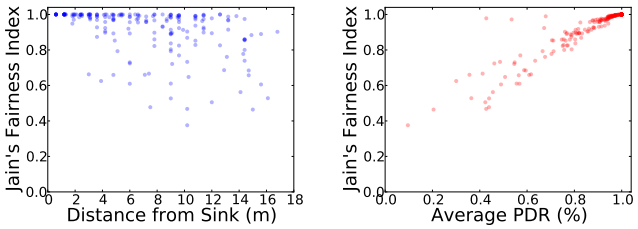
To this aim, we analyzed the PDR performance for all IEEE 802.15.4 radio channels illustrated in Fig. 4. As can be observed, the IEEE 802.11 channels that perform worse correspond to the most commonly used by WiFi-enabled devices (cf. Fig. 1).

Moreover, it is worth mentioning that not all radio links suffer similarly from external interference. In particular, while many links perform badly on channels 12 and 13, some others (e.g., $1.2\ m$, $4.7\ m$) still achieve a perfect reliability (100%). Indeed, short distance links tend to be less sensitive to external interference. Their signal strength may be higher and, consequently, these radio links are more robust.

B. Accuracy of the Link Quality Indicators

To further characterize the links, we focus on a single radio link (i.e., distance of $13.2\ m$, Fig. 5). RSSI and LQI serve as link quality indicators, since the level of the received signal is correlated with the Bit Error Rate (BER). However, these link indicators do not reflect here the actual PDR for each channel.

Indeed, RSSI and LQI can only be measured for correctly decoded packets. With the presence of external interference, some of the packets are corrupted and, thus, are not received correctly. While these dropped packets have an impact on the PDR, RSSI and LQI of the received packets remains unchanged. Thus, hereafter, in order to detect external interference, we explicitly focus on the estimation of PDR.



(a) Impact of the distance on the Channel Jain Index

(b) Channel Jain Index and average PDR correlation.

Fig. 6: Fairness among the different channels

C. PDR Fairness among Channels

We now investigate the variability of bad links and we ask ourselves the following question: is PDR similar for all the physical channels or most packets are dropped because of external interference on *some* of the channels?

To quantify fairness, we measured the Jain Index of the PDR for all the channels. Thus, we define the *Channel Jain Index* of a link l as follows:

$$ChannelJainIndex(l) = \frac{\left(\sum_{c\in\mathcal{C}} Avg_{PDR}\,(c,l)\right)^2}{|\mathcal{C}| * \sum_{c\in\mathcal{C}} Avg_{PDR}(c,l)^2} \quad (1)$$

with $\mathcal{C}$ being the set of channels and $Avg_{PDR}(c,l)$ the average PDR for the link l on channel c.

Fig. 6a illustrates the distribution of the Jain Index of the different links according to their euclidean length. This result corroborates our observation about the variability; the links in the gray zone exhibit very different characteristics. In particular, some radio links may perform very differently on all the channels: external interference is present on *some* channels, which implies a bad Channel Jain Index. Furthermore, the distance of radio links seems also correlated with fairness since the probability for a given link to behave differently on the different channels is higher for longer distance links.

Figure 6b illustrates the strong correlation between PDR and fairness. Surprisingly, bad radio links indicate very strong unfairness. In other words, radio links with a low average PDR suffer from packet drops unfairly on *some* channels. Thus, most links with a bad PDR exhibit a very high channel variability. Our conclusion is that blacklisting the bad channels may help them to improve their average link quality.

VI. Time Variability Characterization

We then studied the time variability of the link quality. Indeed, we performed an experiment during 24 hours, where 6 M3 nodes transmit to one single receiver, in a 1-hop star topology with different distances.

We identified two classes of links (stable $vs.$ variable). Due to lack of space, we do not provide the graphs for stable, good links in which all channels perform similarly with very high PDR.

We actually focused on a scenario that considers link distance of 9 m (Fig. 7). More specifically, some of the physical channels perform very well and are very stable (e.g., channels 17, 22, 24, 26), while some other exhibit a very high variability. Furthermore, it is worth mentioning that for example channel 14, should be blacklisted globally, since it provides a bad PDR during the whole experiment (i.e., 24 h). On the contrary, channel 11 could be utilized during hours 02 to 04 and blacklisted between hours 14 to 16.

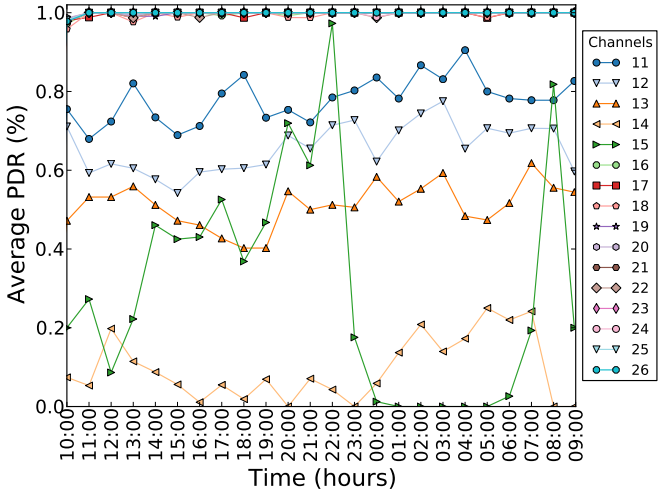


Fig. 7: The variability of the link quality over time: studied case of 9 m distance.

These results **advocate the relevance of a dynamic blacklisting method** in which the network must reactively discover the bad channels and should recover when a channel restarts to perform accurately. Moreover, links seem relatively stable for long periods (i.e., 1 h) and justify the decision to only temporarily blacklist a channel.

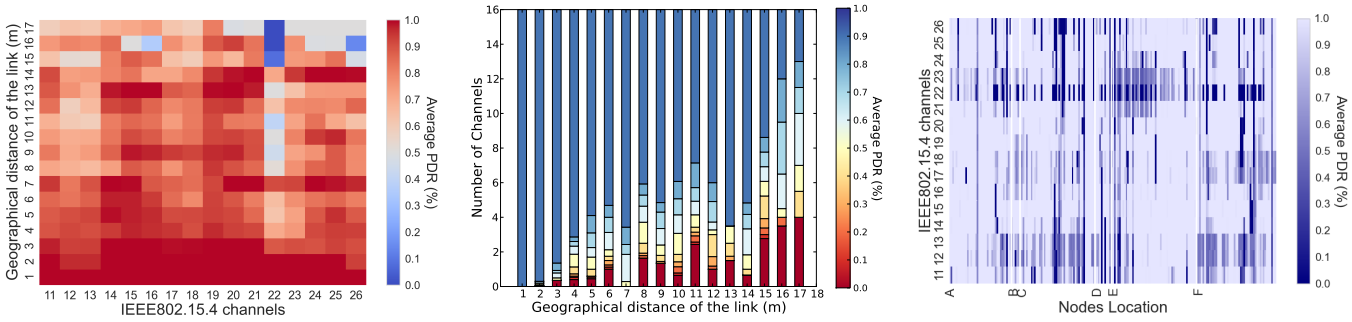
VII. Towards Blacklisting Techniques

In this Section, we study the relevance of the different blacklisting techniques. Thus, we first measured the PDR through each physical channel for different pairs of nodes selected randomly. We then grouped the pairs with similar geographical distance. Fig. 8a illustrates the heat-map of the PDR for different channels and links of a similar quality.

As it can be observed, channel 22 performs badly for almost all radio links. For instance, the PDR of long links (11m) is reduced by 50%, compared to the channel 19 with a reliability over 95%. However, even this channel should not be blacklisted globally, since the shortest links keep achieving a perfect PDR performance. As a result, blacklisting a channel globally decreases network capacity vainly by $\frac{100}{16}\%$.

Furthermore, we can isolate some local patterns. For instance, channels 15 and 16 provide a low PDR only in *some* locations (i.e. a few radio links present in a given geographical area have a low PDR for this channel).

Fig. 8b illustrates the amount of bad/good channels depending on the geographical distance between the transmitter and the receiver. If the distance of the receiver is higher, the unfairness becomes more intensive. We also observe that when the distance is equal to 17 meters, some channels perform very well, while the other ones provide a very low reliability. Thus, this behavior **advocates the usage of a local blacklist**.



(a) Heatmap: average link quality through each channel depending on the radio link geographical length

(b) Classification of the link qualities for different geographical lengths

(c) Heatmap of the PDR for each channel, links being grouped by their geographical location

Fig. 8: Variability of the list of *bad* channels.

Alternatively, the controller may blacklist a channel in a given geographical area. We measured the PDR for each channel according to the location of the links (Fig. 8c). We can remark a semi-global pattern; channel 22 performs badly for a set of radio links, wherever they are located. However, it seems to impact only the weakest links. On the other hand, we can isolate some additional local patterns: in the corridor EF, a few channels seem more perturbed by external interference (channels 21-24). However, the rest of the channels perform on average better than in the other corridors.

VIII. Conclusions & Future Work

In this paper, we first experimentally studied an IEEE 802.15.4-TSCH network by employing the OpenWSN stack to characterize the radio link quality in an indoor environment, such as the FIT IoT-LAB platform. We investigated the time variability of the radio link quality characteristics, and particularly the dependency on the physical channel. Moreover, we studied the geographical dependency of the list of bad radio channels.

We then have studied the characteristics of a possible blacklist (i.e., global versus local) and of bad channels for indoor environments. Indeed, a slow channel hopping MAC helps to combat external interference, limiting consecutive packet drops. However, the channels that always perform *bad* should be blacklisted. Based on our experimental results, we highlighted local characteristics in which some channels perform poorly only for a subset of the radio links. The signal strength and the location of external interference impact significantly the list of channels that perform badly. In conclusion, the list of blacklisted channels should be probably localized, specifically for a zone or a radio link.

In our future work, we plan to propose and evaluate new and adaptive blacklisting techniques. In particular, a central controller should blacklist a bad channel in a given area, while detecting and reacting to channels that perform badly only for a small subset of radio links or a certain period of time.

References

[1] G. Z. Papadopoulos, T. Matsui, P. Thubert, G. Texier, T. Watteyne, and N. Montavont. Leapfrog Collaboration: Toward Deterministic and Predictable in Industrial-IoT applications. In *ICC*. IEEE, 2017.

[2] 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.

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

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

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

[6] A. Cerpa, J. L. Wong, L. Kuang, M. Potkonjak, and D. Estrin. Statistical Model of Lossy Links in Wireless Sensor Networks. In *IPSN*. IEEE/ACM, 2005.

[7] A. Cerpa, J. L. Wong, M. Potkonjak, and D. Estrin. Temporal Properties of Low Power Wireless Links: Modeling and Implications on Multi-Hop Routing. In *MOBIHOC*. ACM, 2005.

[8] G. Z. Papadopoulos, J. Beaudaux, A. Gallais, T. Noel, and G. Schreiner. Adding value to WSN simulation using the IoT-LAB experimental platform. In *WiMob*. IEEE, 2013.

[9] T. Watteyne, C. Adjih, and X. Vilajosana. Lessons Learned from Large-scale Dense IEEE802.15.4 Connectivity Traces. In *CASE*. IEEE, 2015.

[10] T. Watteyne, A. Mehta, and K. Pister. Reliability through frequency diversity: Why channel hopping makes sense. In *PE-WASUN*. ACM, 2009.

[11] WirelessHART Specification. 75: Tdma data-link layer. *HART Communication Foundation Std., Rev*, 1, 2008.

[12] ISA-100.11a-2011:. Wireless systems for industrial automation:process control and related applications. *International Society of Automation (ISA) Std.*, 1, May 2011.

[13] S. Petersen and S. Carlsen. Wirelesshart versus isa100.11a: The format war hits the factory floor. *IEEE Industrial Electronics Magazine*, 5(4):23–34, Dec 2011.

[14] M. Hänninen, J. Suhonen, T. D. Hämäläinen, and M. Hännikäinen. Link Quality-Based Channel Selection for Resource Constrained WSNs. In *GPC*. Springer, 2011.

[15] B. Pavkovic, F. Theoleyre, D. Barthel, and A. Duda. Experimental Analysis and Characterization of a Wireless Sensor Network Environment. In *PE-WASUN*. ACM, 2010.

[16] M. Sha, G. Hackmann, and C. Lu. Arch: Practical channel hopping for reliable home-area sensor networks. In *RTAS*. IEEE, 2011.

[17] P. Du and G. Roussos. Adaptive time slotted channel hopping for wireless sensor networks. In *CEEC*. IEEE, Sept 2012.

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