HAL
open science

Blacklisting-Based Channel Hopping Approaches in Low-Power and Lossy Networks

Vasileios Kotsiou, Georgios Papadopoulos, Dimitrios Zorbas, Periklis Chatzimisios, Fabrice Theoleyre

To cite this version:

Vasileios Kotsiou, Georgios Papadopoulos, Dimitrios Zorbas, Periklis Chatzimisios, Fabrice Theoleyre. Blacklisting-Based Channel Hopping Approaches in Low-Power and Lossy Networks. IEEE Communications Magazine, 2019, 57 (2), pp.48-53. 10.1109/MCOM.2018.1800362 . hal-02323140

HAL Id: hal-02323140

https://hal.science/hal-02323140

Submitted on 29 Jan 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Blacklisting-based Channel Hopping Approaches in Low-power and Lossy Networks

Vasileios Kotsiou, Georgios Z. Papadopoulos, *Member, IEEE,* Dimitrios Zorbas, *Member, IEEE,* Periklis Chatzimisios, *Senior Member, IEEE,* and Fabrice Théoleyre, *Senior Member, IEEE*

***Abstract*— More and more industrial applications require high reliability, while relying on low-power devices for their flexibility. Unfortunately, radio transmissions are prone to unreliability, and are very sensitive to external interference. Therefore, a great amount of effort has been put on channel hopping approaches, which help to combat external interference by reducing the number of packet losses. This approach is combined with a strict schedule of the transmissions to allow the devices to save energy. However, some of the radio channels are subjected to strong interference. Blacklisting techniques identify the interfered radio channels that demonstrate low packet delivery radio and avoid using them to transmit data packets. In this article, we study different distributed and global blacklisting techniques and investigate their dependencies on the scheduling algorithm. We also present a new scheme to exploit a blacklist by making the employed scheduling algorithm blacklist-aware. Our results rely on a real experimental dataset to quantify the performance of all these approaches and demonstrate the interest of blacklisting to improve network reliability.**

***Index Terms*—slow channel hopping; Internet of Things; Blacklisting; reliability; low-power and lossy networks**

I. Introduction

Smart City applications rely extensively on the Internet of Things (IoT), requiring network reliability above 99.9% and guaranteed maximum delay and jitter. For instance, smart parkings need to collect real time information to provide a good quality of experience [1].

To fulfill these requirements, the IEEE 802.15.4-TSCH standard [2] relies on a fixed schedule of transmissions to enable deterministic communication. A set of *cells* (timeslot and channel offset) is allocated to each radio link, denoting when and through which radio channel the packets have to be transmitted. By accurately allocating different channel offsets to interfering links scheduled in the same timeslot, the wireless network can provide delay and reliability guarantees. The network maintains a global clock which typically counts the number of timeslots, i.e., Absolute Sequence Number (ASN), since the network is bootstrapped.

The level of external interference has been proved to be high in smart building scenarios, with several co-located networks [3]. Radio channel hopping enables to combat the external interference, deriving the frequency to use from the channel offset and the ASN. Thus, a packet and its retransmissions do not use the same physical frequency, making packet failures less repetitive.

V. Kotsiou and F. Theoleyre are with the ICube lab, CNRS / University of Strasbourg; G. Z. Papadopoulos is with the IRISA, IMT Atlantique, France; D. Zorbas is with the Tyndall National Institute, Ireland; P. Chatzimisios is with Alexander TEI of Thessaloniki and Bournemouth University, UK.

[0]IEEE ©2018 http://dx.doi.org/10.1109/MCOM

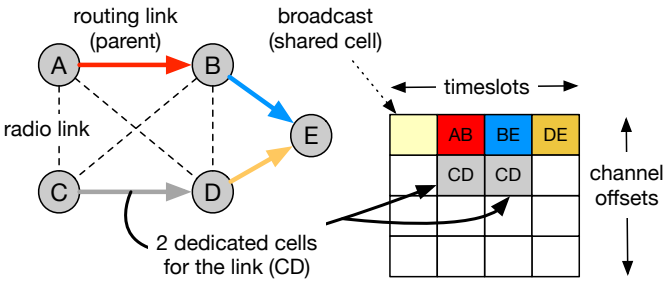

Fig. 1: A 5-node topology with a simple TSCH schedule using dedicated cells for the (unicast) data transmissions.

However, external interference increases the number of retransmissions. Thus, blacklisting aims to identify the *bad* radio channels, which exhibit a low PDR, and to modify the radio channel hopping sequence accordingly. While routing, scheduling and blacklisting could be optimized together [4], the problems are often considered independently due to time complexity issues.

The assignment of the timeslots and channel offsets can be achieved by a centralized controller or node by node distributively in the network. In Fig. 1, a typical schedule is illustrated: it consists of a matrix of channel offsets and timeslots (a slotframe), which repeats indefinitely over time. Certain transmission opportunities are allocated for broadcast packets (e.g., control packets) in contention-based manner, where all nodes have to stay awake, while other cells are allocated per link for unicast packets, in a collision-free manner.

To cope with unreliable links, the network has to perform an over-provision of a set of cells for retransmissions. Unfortunately, these retransmissions have a negative impact on end-to-end delay and jitter, and reduce the network capacity.

The contributions of this paper are as follows:

1) We provide experimental results relying on IEEE 802.15.4-TSCH to justify the relevance of blacklisting for slow channel hopping;
2) We discuss and quantify the assets and limits of implementing a global (common to all the devices) versus a local (specific to a given radio link) blacklisting technique;
3) We provide additional open challenges in this research

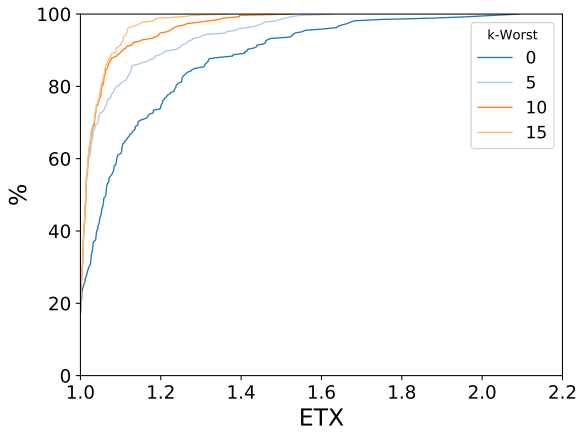

Fig. 2: CDF of the ETX value for all the radio links.

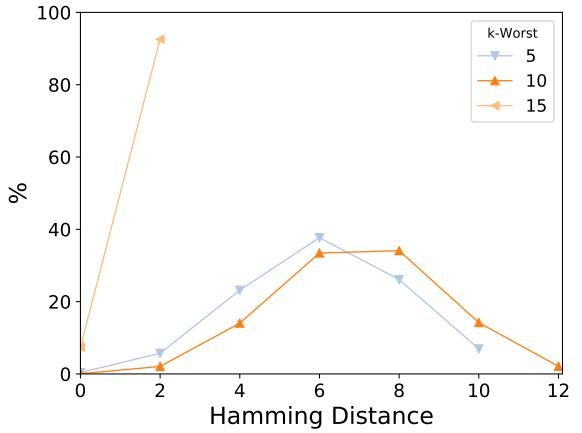

Fig. 3: Heterogeneity in the blacklists.

area.

II. Why is blacklisting still required for channel hopping?

One may argue that radio channel hopping is sufficient since frequency diversity allows to reduce the number of repetitive failures. However, not all frequencies exhibit similar characteristics. In that case, over-provisioning may improve the end-to-end reliability, but it impacts negatively the energy consumption and the network capacity. Hereafter, we will provide experimental results to defend the relevance of blacklisting techniques to avoid these unnecessary retransmissions.

A. Experimental dataset

We focus here on a smart building scenario where a set of sensors periodically sends measurements to a border router (aka. Constant Bit Rate flows). For this purpose, we emulate this scenario on the FIT IoT-LAB platform (https://www.iot-lab.info/). The experiments rely on IEEE 802.15.4-TSCH (with the http://openwsn.org open-source implementation), since it represents a popular industrial standard implementing a channel hopping approach.

To mimic a smart building environment, we collect a large dataset of measurements to emulate real link qualities. We store the packet success / failure for 267 radio links, with one packet every 3 seconds, during 90 min. The distance between the transmitter and receivers varies from 0.6 to 17 m [3], [5]. We have co-located WiFi, and other concurrent experiments, which generate external interference. We inject this dataset in a custom made Python simulator, to decide if a packet is received or dropped because of external interference. We focus here on the efficiency of blacklisting in single hop topologies.

Several techniques have been proposed in the literature to construct a blacklist with a fixed [6], [7] or variable [5] size. For the sake of simplicity, we focus here uniquely on fixed-size blacklists, utilizing the two following strategies:

1) **k-Worst Channels:** This blacklisting technique excludes from the channel hopping sequence the k-worst radio channels with the poorest Packet Delivery Ratio (smoothed with a WMEWMA estimator [7]).
2) **Default:** We do not exclude any radio channel from the channel hopping sequence (equivalent to k=0).

B. Blacklist Efficiency

We first measure the Cumulative Distribution Function (CDF) of the Expected Transmission Count (ETX) value for all the links when blacklisting a different number of radio channels (Fig. 2). The ETX metric counts the average number of packets to transmit before receiving an acknowledgement. Without blacklisting (k=0), ETX is high, denoting retransmissions; some radio channels perform badly and impact significantly reliability. On the contrary, blacklisting automatically removes the bad radio channels from the frequency hopping sequence, thus, we need less retransmissions on average. This improvement has a counter-part: the network capacity is reduced since the network can only exploit a smaller number of radio channels.

C. Blacklist changes

In a global blacklist scheme, the controller typically collects continuously the link quality metric to cope with time-variable conditions. If the radio channel quality changes significantly, the blacklist is updated and pushed to all the nodes. Similarly, per-link blacklists may change if the Packet Delivery Ratio (PDR) per radio channel evolves. Then, the transmitter has to notify the receiver of the novel blacklist.

D. Location-based Heterogeneity

We explore the location-dependent characteristics of the different blacklists, by comparing pair-wisely the blacklists of different links (see Fig. 3). We use the Hamming Distance, counting the number of positions where the bits differ for a pair of binary strings. Here, we associate a 16-bit string to each link, the ith bit being set to 1 if the radio channel i is blacklisted. In our case, the Hamming distance counts the number of radio channels which differ in the two blacklists.

We note that the Hamming distance is an absolute metric. In particular, two very long blacklists (e.g., 15) can only differ by

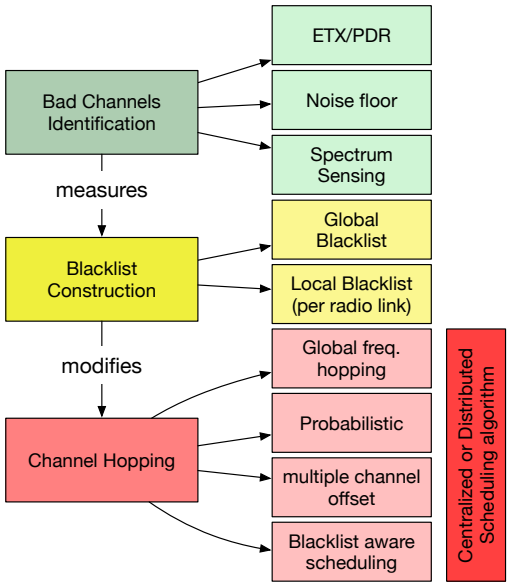

Fig. 4: Taxonomy and Components of the Blacklist Construction and Exploitation

one radio channel, leading to an Hamming distance at most equal to 2. However, a global blacklist would be inefficient even in that case: selecting randomly one pair of radio link, we have a 90% probability that the best radio channel differs.

Blacklists with 5 radio channels are very different: 50% of pairs of links share less than one half of the radio channels. In other words, the blacklist is very location dependent and, thus, radio links have different blacklists. Consequently, relying on the same blacklist in the whole network would be suboptimal.

III. Blacklisting Approaches for Slow Channel Hopping

We follow the following steps to exploit a blacklist in channel hopping networks (Fig. 4):

1) We identify the bad radio channels based on a channel quality metric;
2) We construct a blacklist which may be global (common to all nodes) or local (specific to each radio link);
3) We modify the pseudo-random sequence to limit the usage of the blacklisted radio channels.

We note that the scheduling approach (distributed vs. centralized) also impacts the way to modify the radio channel hopping sequence. We will now detail each step of this process.

A. Identifying bad radio channels

A *bad* radio channel is a frequency whose usage increases globally the number of retransmissions and impacts negatively the network reliability [8]. Thus, a bad radio channel exhibits a high number of retransmissions compared to the other ones. Moreover, a *bad* radio channel may provide a high PDR for *some* links while its usage increases *globally* the number of retransmissions. Typically, such radio channel should be removed from the hopping sequence.

Most heuristics identify the radio channels providing a poor reliability by measuring the average ETX value independently for each radio channel [7]. Alternatively, more sophisticated techniques may be implemented to detect the bad radio channels, measuring the noise floor (which should be on average higher for *bad* radio channels), or a spectrum sensing method [6]. RSSI has been proved to reflect very loosely the link quality [3].

Alternatively, ETSCH applies a non-intrusive radio channel quality estimation by performing energy detection during idle periods of any timeslot [9]. This technique is efficient when the timeslot duration is sufficient to compensate clock drifts, while letting enough time for energy detection. Addressing multi-hop topologies is still an open challenge and dedicated timeslots for energy detection may be required.

B. Blacklists Construction

1) Global blacklists: Several standards rely on global blacklisting to avoid using the bad radio channels: a radio channel which presents poor characteristics in the whole network is removed from the hopping sequence. Since it corresponds to a global consensus, most of the implementations are centralized: a controller collects all the statistics and decides which frequencies to blacklist. Then, the hopping sequence is typically piggybacked in the periodical beacons to push the configuration to all the nodes.

Constructing the blacklist corresponds to an optimization problem. For instance, one may select a blacklist which minimizes the maximum number of retransmissions for all the radio links to consider fairness. Alternatively, an heuristic where the controller blacklists the k radio channels with the worst PDR allows the network to remove the radio channels which provide *on average* a poor reliability.

2) Local blacklists: Alternatively, the devices can locally decide if a radio channel is bad for a specific radio link. Most of the approaches propose to blacklist all the radio channels with a metric below (or above) a given threshold value. For instance, Du *et al.* [10] consider the RSSI value of each radio channel, measured during *quiet* intervals for which transmissions are forbidden.

Since the blacklist is constructed locally, the receiver and the transmitter have to construct a common list of radio channels to exclude for their transmissions. Otherwise, inconsistent blacklists would lead to deafness. Du *et al.* [10] propose to piggyback the blacklist in the `beacons`. Unfortunately, `beacons` are not acknowledged, and inconsistencies may still arise. Gomes *et al.* [11] propose rather to piggyback the blacklist in the `data` and `ack` frames while maintaining a *blacklist sequence number*. The transmitter uses the blacklist that corresponds to the highest sequence number acknowledged by the receiver.

C. Channel Hopping modification

At the beginning of a timeslot, a device verifies in the schedule if it has to stay awake. If the cell is allocated to the device, the physical frequency to use for transmission/reception is derived from the ASN of the timeslot and the channel offset

assigned to this cell. More precisely, it sums the ASN value and the channel offset assigned to the links, and then applies a modulo operator to map this integer to a frequency from the hopping sequence.

Thus, exploiting a blacklist means to modify the frequency hopping sequence to remove or use less frequently the bad radio channels. Since very different (and mainly incompatible) approaches exist in the literature, we detail each of them in the next section.

IV. Exploiting a Blacklist: Changing the Frequency Hopping Sequence

After having identified the bad radio channels, next we have to modify the frequency hopping sequence. This modification may be applied globally for all the nodes and cells. Alternatively, a per-link hopping sequence may be defined. In that case, it only applies to the dedicated cell, where a specific receiver is identified.

A. Global common frequency hopping sequence

When the blacklist is global, all devices have to modify their pseudo-random hopping sequence. It practically means that each device has to adjust the number of available channel offsets to contain only the number of non-blacklisted radio channels so the physical mapping function gives only the *good* radio channels.

The blacklist may be piggybacked in the Enhanced Beacons (EB): a node that joins the network extracts the blacklist from the EB and constructs accordingly the frequency hopping sequence. In adaptive solutions, the blacklist must be updated to reflect the actual performance of the network. In a centralized approach, the centralized controller must collect the statistics for each radio link and then identify the radio channels which perform badly. The nodes should start using a blacklist only when all of them received the new version [12]. Otherwise deafness and even network disconnection may occur.

B. Probabilistic assignment

A device should use more frequently the good radio channels to reduce the average number of retransmissions. Thus, the transmitter can remove the bad radio channels from its frequency hopping sequence. However, collisions may arise in this case even among two interfering links that use a different channel offset.

Let us consider the example depicted in Fig. 5 (single offset case) with the same topology as Fig. 1. Let us assume that nodes (A, B) (resp. (C, D)) have blacklisted radio channels 13-15 and 20-23 (resp. 19-23). Given a value of ASN=50, we can observe that the mapping function will generate the same radio channel for both nodes and, thus, the corresponding transmissions will collide, i.e., collisions due parallel transmissions.

To make the collisions less repetitive, a device spreads the load pseudo-randomly on all the good radio channels [5]. The frequency to use depends on the result of the frequency mapping function:

Good radio channel: the device uses it in the current timeslot;

Bad radio channel: the device uses a radio channel selected pseudo-randomly among the good ones. Practically, it re-applies the frequency mapping function after having incremented a common variable (ID of the transmitter) until the result corresponds to a good radio channel.

Sha et al. [13] detail a mechanism to decrease the computation cost for adaptive blacklisting, avoiding to regenerate from scratch the sequence when the blacklist has changed. However, both approaches consider single hop topologies, although avoiding collisions in multi-hop scenarios with a probabilistic approach is still an open problem.

This probabilistic approach keeps on generating collisions. While these collisions are not repetitive, they impact the reliability, particularly with dense networks using long and heterogeneous blacklists.

C. Multiple channel offsets assignment

The network may allocate one timeslot and several channel offsets to a given link, such as MABO-TSCH does [11]. The blacklist can then be negotiated locally, among the transmitter and the receiver. At the beginning of a timeslot, a node uses its channel offsets list to derive the frequency to use. More precisely, if the first channel offset corresponds to a blacklisted radio channel, it uses the next channel offset in its list. The process stops when a good radio channel is obtained, or the last channel offset is scanned.

This method is illustrated in Fig. 5 (multi-offset case). The link (A, B) received three different channel offsets. The first channel offset (1) gives a bad radio channel and is not used. Finally, only the third channel offset corresponds to a good radio channel, which will be used for the transmission.

This strategy does not create any collision; the channel offsets are distributed orthogonally (a pair of interfering links never receives the same channel offset). However, a fixed (small) number of channel offsets is assigned to each link. With long blacklists, we will keep on using poor radio channels, impacting negatively reliability. An adaptive strategy, to decide on the optimal number of channel offsets to assign per link, has still to be proposed.

This multi-channel offset scheme supports both centralized and distributed scheduling algorithms: a link has just to reserve several channel offsets. However, the detection of collisions with a distributed scheduling algorithm is more complicated. Since several channel offsets are used, the collisions will not occur when two links share *one part* of the channel offsets.

D. Blacklist-aware assignment

Since this approach has not been studied so far, we propose here the first blacklist-aware centralized scheduling algorithm. To the classical constraints (half-duplexity, interference, etc.) [14], we insert a set of constraints to deal with blacklists:

Same blacklist: If two radio links have the same blacklist, they cannot create collisions if they are allocated in the same timeslot with different channel offsets. The mapping function will never give the same result;

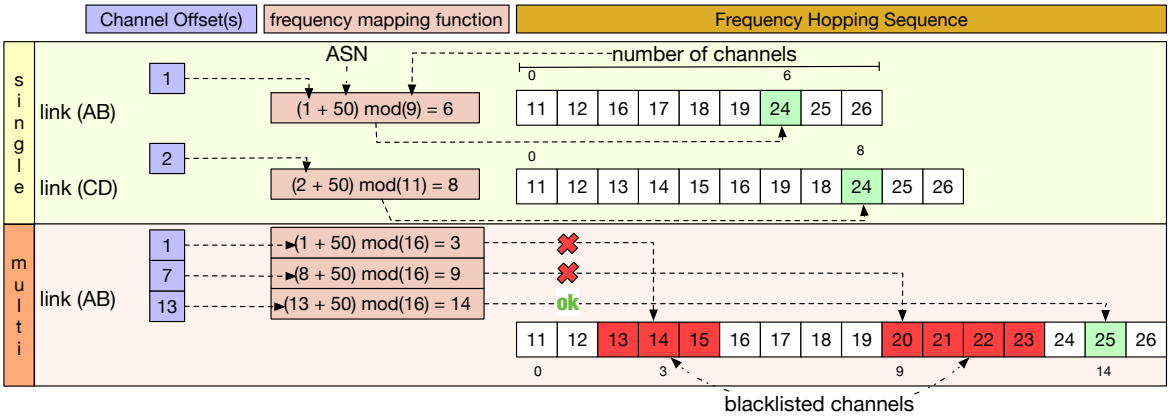

Fig. 5: Selection of the frequency from the channel offset(s)

Disjoint whitelist: Whitelists represent the complement of blacklists. If two radio links use a disjoint whitelist, no collision can take place by definition.

In all other cases, the scheduling algorithm considers a blacklist conflict and allocates different timeslots to the two links.

The centralized controller needs to know the blacklist of all the links, which may represent a large overhead. Adaptive blacklists mean that the schedule has to be probably changed accordingly, since new blacklisting constraints may arise.

Conflicting links are scheduled in different timeslots, and the schedule length tends to increase when blacklists are very different among the nodes. We need to explore how the centralized controller can also tune the blacklists to reduce the number of constraints. For instance, a frequency may be inserted by the centralized controller in a blacklist if it removes the conflict between a pair of links.

V. Performance Evaluation

A. Simulation Methodology

To efficiently mimic a smart building scenario, we have to construct multi-hop topologies. We generate random topologies of 40 nodes and one root, randomly positioned in an area of 200 X 200 m^2, the coverage range of each node is 50 m [14]. The average number of neighbors per node is 6.5. and the average number of hops is 3.07 (maximum 6).

We then adopt the same methodology as described in Section II-A to map a simulated link to a link from the dataset. When a packet is generated, the transmission success / failure is derived from the dataset with the correct physical frequency used for the transmission. This way, we are able to emulate external interference.

A gradient based routing as IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is executed, and a node selects as parent its neighbor closest from the sink. Besides, the construction of the schedule was carried out using the Traffic Aware Scheduling Algorithm (TASA) [14]. A node generates a random number of packets (comprised between [1,5]) at the beginning of each slotframe. We consider 16 channel offsets and a slotframe size of 293 timeslots to support all the flows and their possible retransmissions. We repeat each experiment for ten different random network topologies.

We measure the following metrics:

- **Link-level PDR:** Ratio of the number of data packets delivered by the receiver and the total number of data packets transmitted by the transmitter;
- **Percentage of Collisions due to parallel transmissions:** Ratio of the number of colliding packets due to parallel transmissions and the total number of transmitted packets by all the nodes.

B. Evaluation

We compare the following solutions:

- **Default**: no radio channel is blacklisted;
- **Global**: each radio link ranks its radio channels according to their PDR, the rank being its position in the list. We blacklist globally the k radio channels that provide the lowest *average* PDR for all the links;
- **Local**: to compare fairly the global and local approaches, we blacklist the k worst radio channels for each radio link. Then, we implement the following approaches:
  - **Probabilistic**: similar to [5] (section IV-B);
  - **Multiple**: similar to MABO-TSCH [11] (section IV-C);
  - **Blacklist-aware**: our proposed centralized blacklist aware scheduling approach (section IV-D). Since we let each radio link to continuously update its blacklist dynamically, some collisions may arise among different channel offsets.

We measure the PDR obtained at the link level (Fig. 6). The default approach does not use blacklisting and, thus, many retransmissions occur: only 85% of the packets are acknowledged correctly. The global blacklist improves the packet delivery ratio, blacklisting the radio channel which performs the worst for some links. However, long blacklists lead to a smaller network capacity, since the load has to be spread over a small number of frequencies. The reliability increases with longer blacklists for the probabilistic approach: the number of collisions is negligible; using better radio channels is always advantageous. On the contrary, the reliability decreases for the multichannel offset approach: longer blacklists imply that we have to allocate a very large number of channel offsets

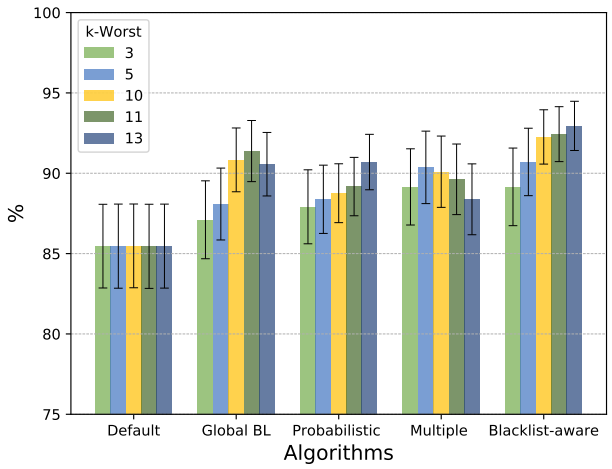

Fig. 6: Link-level Packet Delivery Ratio.

for each link, decreasing the efficiency. Finally, the blacklist-aware assignment seems the most efficient, since it adapts the schedule in a centralized way while tuning the blacklist locally.

VI. Open Challenges

We have demonstrated the relevance of using blacklisting to reduce the number of transmissions, which impact negatively both the reliability and the energy consumption. However, there are still certain open issues when exploiting blacklists:

Joint-optimization: Considering the routing, scheduling, and blacklisting all together may help to improve performance. For instance, the scheduling algorithm may decide to change the blacklist to relax the scheduling constraints. We have first to investigate theoretically the gap to fill between a disjoint and a conjoint optimization. Then, heuristics have to be proposed if this gap is significant;

Capacity reduction: With longer blacklists, the nodes reduce the usage of bad radio channels and, thus, the number of retransmissions. However, transmissions have to be multiplexed through a smaller number of radio channels, increasing the probability of collisions in dense networks. An adaptive blacklist size, which optimizes reliability while respecting a minimum network capacity has still to be proposed.

Co-located networks: Blacklisting has been designed for external interference using a static set of radio channels. If other co-located networks adopt a channel hopping strategy, blacklisting would be inefficient since the load is spread uniformly across all the radio channels [15]. We should rather be able to detect interfering networks adopting the same strategy, for instance with a classification technique. Then, an heuristic to share the radio spectrum among the interfering networks shall be proposed.

VII. Conclusion and Perspectives

A channel hopping based MAC protocol helps to combat external interference but it is still insufficient. Blacklisting techniques identify the radio channels which exhibit a poor reliability and modify the behavior of the link layer to use mostly the best radio channels. We investigated here the negative impact of long blacklists on the network capacity, specifically for global blacklists. We also detailed how the scheduling algorithm is tightly dependent on the blacklisting technique.

Centralized scheduling algorithms with a global blacklist have still to be evaluated under real conditions: obtaining the statistics (link reliability, amount of packets) in real time corresponds to a challenging objective. Single channel MAC also needs to identify the *best* radio channel to use for the whole network. A common consensus is here required similar to a global blacklisting problem. In particular, non-intrusive channel quality estimation techniques may be re-adapted to tackle this problematic.

References

[1] K. Kritsis, G. Z. Papadopoulos, A. Gallais, P. Chatzimisios, and F. Théoleyre, "A tutorial on performance evaluation and validation methodology for low-power and lossy networks," *IEEE Communications Surveys & Tutorials*, vol. 20, pp. 1799–1825, March 2018.

[2] IEEE Standard for Low-Rate Wireless Networks, "IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)," April 2016.

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

[4] D. Gunatilaka, M. Sha, and C. Lu, "Impacts of Channel Selection on Industrial Wireless Sensor-Actuator Networks," in *Proc. of the IEEE International Conference on Computer Communications (INFOCOM)*, 2017.

[5] V. Kotsiou, G. Z. Papadopoulos, P. Chatzimisios, and F. Theoleyre, "LA-BeL: Link-based Adaptive BLacklisting Technique for 6TiSCH Wireless Industrial Networks," in *Proc. of the 20th International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM)*. ACM, 2017.

[6] F. Chiti, R. Fantacci, and A. Tani, "Performance Evaluation of an Adaptive Channel Allocation Technique for Cognitive Wireless Sensor Networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 5351–5363, June 2017.

[7] C. F. Shih, A. E. Xhafa, and J. Zhou, "Practical frequency hopping sequence design for interference avoidance in 802.15.4e TSCH networks," in *Proc. of the IEEE International Conference on Communications (ICC)*, 2015.

[8] D. Zorbas, V. Kotsiou, F. Théoleyre, G. Z. Papadopoulos, and C. Douligeris, "LOST: Localized Blacklisting Aware Scheduling Algorithm for IEEE 802.15.4-TSCH Networks," in *Proc. of the 10th Wireless Days (WD)*, 2018.

[9] R. Tavakoli, M. Nabi, T. Basten, and K. Goossens, "Enhanced Time-Slotted Channel Hopping in WSNs Using Non-intrusive Channel-Quality Estimation," in *Proc. of the IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2015.

[10] P. Du and G. Roussos, "Adaptive channel hopping for wireless sensor networks," in *Proc. of the International Conference on Selected Topics in Mobile and Wireless Networking (iCOST)*, 2011.

[11] P. H. Gomes, T. Watteyne, and B. Krishnamachari, "MABO-TSCH: Multi-hop And Blacklist-based Optimized Time Synchronized Channel Hopping," *Transactions on Emerging Telecommunications Technologies*, vol. e3223, pp. 1–20, 2017.

[12] D. Zorbas, G. Z. Papadopoulos, and C. Douligeris, "Local or Global Radio Channel Blacklisting for IEEE 802.15.4-TSCH Networks?" in *Proc. of the IEEE International Conference on Communications (ICC)*, 2018.

[13] M. Sha, G. Hackmann, and C. Lu, "ARCH: Practical Channel Hopping for Reliable Home-Area Sensor Networks," in *Proc. of the 17th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)*, 2011.

[14] M. R. Palattella, N. Accettura, L. A. Grieco, G. Boggia, M. Dohler, and T. Engel, "On Optimal Scheduling in Duty-Cycled Industrial IoT Applications Using IEEE802.15.4e TSCH," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3655–3666, Oct 2013.

[15] S. B. Yaala, F. Theoleyre, and R. Bouallegue, "Cooperative Resynchronization to Improve the Reliability of Colocated IEEE 802.15.4-TSCH Networks in Dense Deployments," *Ad Hoc Networks*, vol. 64, pp. 112 – 126, 2017.

BIOGRAPHIES

VASILEIOS KOTSIOU (kotsiou@unistra.fr) is a Ph.D. student at the ICube laboratory, University of Strasbourg, France. Previously, he received his M.Sc. in Engineering of Pervasive Computing Systems from Hellenic Open University in 2014 and his B.Sc. in Computer Science from University of Crete (Heraklion) in 1996. He is the author of peer-reviewed papers in international conferences and journals (e.g., IEEE SENSORS, IEEE WF-IoT).

GEORGIOS PAPADOPOULOS [S'10, M'15] (georgios.papadopoulos@imt-atlantique.fr) serves as an Associate Professor at the IMT Atlantique in Rennes, France. Previously, he was a Postdoctoral Researcher at the University of Bristol. He received his Ph.D. from University of Strasbourg, in 2015 with honors (Best Ph.D. Thesis Award). Dr. Papadopoulos has participated in various international and national (FP7 RERUM, FIT Equipex) research projects. He has received the prestigious French national ANR JCJC grant for young researchers. He has been involved in the organization of many international events (AdHoc-Now'18, IEEE CSCN'18). He has been serving as Editor for Wireless Networks journal and Internet Technology Letters.

DIMITRIOS ZORBAS [S', M'] (dzorbas@unipi.gr) holds a PhD in Computer Science from the University of Piraeus in Greece. He has worked as post doctoral researcher at Inria Lille – Nord Europe and at University of La Rochelle in France. He is currently researcher at Tyndall National Institute after receiving a Marie Curie fellowship. He is author of more than 30 peer-reviewed publications in the area of computer communications, energy efficiency in networks, and secure communications. He has also worked in several national as well as FP7 and H2020 projects.

PERIKLIS CHATZIMISIOS [S'02, M'05, SM12'] (peris@it.teithe.gr) received his B.Sc. degree from ATEITHE, Thessaloniki, Greece, in 2000, and the Ph.D. degree in wireless communications from Bournemouth University, U.K., in 2005. He serves as an Associate Professor and the Director of the CSSN Research Laboratory in the Department of Informatics, ATEITHE. He has edited/authored eight books and more than 130 peer-reviewed papers and book chapters. His published research work has received more than 3300 citations. Dr. Chatzimisios is involved in several IEEE boards.

FABRICE THÉOLEYRE [S'05, M'09, SM'16] (theoleyre@unistra.fr) is a researcher at the CNRS, ICube Lab, University of Strasbourg since 2009, after having spent two years at LIG, Grenoble (France). He received his PhD in computer science from INSA, Lyon (France) in 2006. He was a visiting scholar at the University of Waterloo (Canada) in 2006, and at INRIA Sophia Antipolis (France) in 2005. He has been involved in several TPC and editorial boards (e.g. Ad Hoc Networks, IEEE Communications Letters, Computer Communications).