Local or Global Radio Channel Blacklisting for IEEE 802.15.4-TSCH Networks?

Dimitrios Zorbas, Georgios Papadopoulos, Christos Douligeris

Local or Global Radio Channel Blacklisting for IEEE 802.15.4-TSCH Networks?

Dimitrios Zorbas*, Georgios Z. Papadopoulos†, and Christos Douligeris*
*NetLab, Department of Informatics, University of Piraeus, Greece, {dzorbas,cdoulig}@unipi.gr
†IMT Atlantique, IRISA, UBL, France, georgios.papadopoulos@imt-atlantique.fr

***Abstract*—The IEEE 802.15.4 Time Slotted Channel Hopping (TSCH) networks suffer considerably from the high interference caused by the presence of nearby external devices, such as from the presence of IEEE 802.11b/g/n Access Points. Frequency hopping and blacklisting of radio channels that temporarily or consistently present bad performance are the two main approaches to cope with interference and increase the chances of successful packet delivery. However, the blacklisting of a number of channels and the scheduling of transmissions so that two or more neighboring links do not use the same frequency at the same time is a challenging problem, since in IEEE 802.15.4 TSCH many parallel transmissions may occur. Blacklisting algorithms may be applied either locally or globally in IEEE 802.15.4 networks. In this paper, we first present the weaknesses of a localized blacklisting solution presented in the literature for multi-hop networks, and we propose a new distributed solution to overcome these issues. Both analytical and simulation evaluation under heavy interference show the superiority of the proposed scheme. In particular, the packet delivery ratio is improved while achieving minimum delay.**

***Index Terms*—IoT; IEEE 802.15.4; TSCH; Interference; Blacklisting;**

I. Introduction

Industrial applications, such as smart grid, smart manufacturing or automotive industry applications, require ultra low-latency, ultra low-power consumption and high network reliability. However, the conventional wireless technologies are prone to external interferences, which negatively impact the network performance. Therefore, the Industrial Internet of Things (IIoT) concept, that employs IoT technologies to combat the previously presented issues, is being currently examined in both research and application environments. In 2016, the IEEE 802.15.4-Time-Slotted Channel Hoping (TSCH) protocol was standardized to provide strict guarantees for IIoT applications [1]. TSCH provides low-power, deterministic and reliable operations for wireless networks. To mitigate the contention in the wireless medium, TSCH comes with a scheduling based on time-synchronization. Moreover, it employs a channel hopping approach to combat the noisy environments.

All IEEE 802.11, IEEE 802.15.1 and IEEE 802.15.4 standards operate in $2.4GHz$. Thus, most of the IEEE 802.15.4 radio channels heavily suffer from other overlapping $2.4GHz$-based wireless technologies [2], [3], [4], [5]. Indeed, only 15, 20 and 25-26 IEEE 802.15.4 radio channels do not (theoretically) interfere with the broadly used IEEE 802.11 channels, see Fig. 1. For instance, in the WiFi (i.e., IEEE 802.11) technology, the popular radio channels 1, 6 and 11 are the main source of interference and, thus, of the degradation observed in the performance of IEEE 802.15.4 [6], [7].

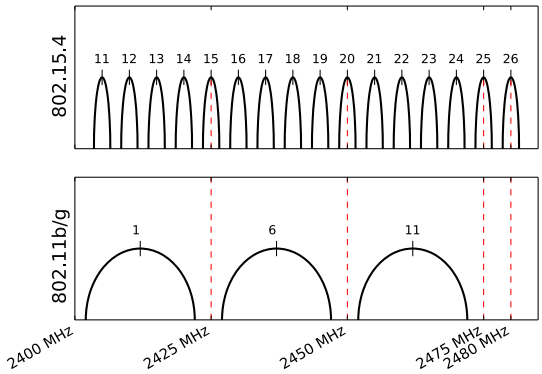

Fig. 1. Interfering radio channels: IEEE 802.15.4 and IEEE 802.11: 1, 6 and 11 are the three non-overlapping and broadly used radio channels for IEEE 802.11 technology.

In such heavily overlapping environments, the channel hopping solution might be insufficient to combat the potential interference. Therefore, the standardization bodies such as IEEE 802.15.4, ISA100.11a [8] and WirelessHART [9], consider the use of blacklisting of the bad radio channels; channels that present bad packet delivery ratios. Kotsiou et al. [10] showed that by employing a blacklisting scheme both network reliability and energy efficiency may improve considerably. Indeed, the blacklisting approach might be applied for the overlapping radio channels that present poor performance for long periods [7]. For instance, WirelessHART comes with a global blacklisting approach, i.e., globally removing the bad channels from the frequency hopping sequence [11], while ISA100.11a supports a local blacklisting approach.

The current blacklisting solution for multi-hop IEEE 802.15.4 TSCH networks [12] is based on a centralized multi-offset assignment. These multiple channel offsets are used to increase the chances of generating a channel that has good performance as well as to avoid frequency overlapping with neighbors transmitting at the same time. However, as we analyze later in the paper, there is a high probability none of the assigned offset to produce an available frequency, especially when many channels have already been blacklisted. In this paper, we tackle this issue by introducing a global blacklisting approach using a single channel offset and by distributing the bad channels to the entire TSCH network.

The contributions of this paper are as follows:

1) We theoretically show that the local-based blacklisting technique presented in the literature may cause significant packet delays when many channels are blacklisted and a few channel offsets are assigned.
2) We present a distributed global blacklisting method to overcome the local blacklisting issues.
3) Finally, our performance evaluation under IEEE 802.11 interference demonstrates that the proposed global blacklisting approach reduces delay and increases the Packet Delivery Ratio (PDR) up to 98%.

II. Background and Related work

A. IEEE 802.15.4-TSCH

In TSCH-based networks, time is slotted into timeslots of equal length, where a set of timeslots constructs a slotframe. During a timeslot a pair of nodes may transmit a data packet and receive an acknowledgement or they may turn their radio `off` for energy saving purposes. The timeslots can be either contention-free dedicated for unicast communication or contention-based, i.e., shared cells for broadcast transmissions. An Absolute Sequence Number (ASN) is tagged in each timeslot to count the number of timeslots since the TSCH network was initiated.

Furthermore, TSCH comes with a channel hopping solution to mitigate the impact of the external interferences. It is worth mentioning that the TSCH schedule is a matrix that consists of timeslots and channel offsets, i.e., cells. Each channel offset is converted into an actual radio channel as follows:

$$CH = \texttt{map}\,[ASN + channel\_offset]\ \texttt{mod}\ nFreq, \quad (1)$$

where $channel\_offset$ is the channel offset, $nFreq$ is the number of available (non-blacklisting) channels (i.e., 16 when using IEEE 802.15.4-compliant radios at 2.4 GHz with all channels in use), and `map` a bijective function mapping an integer between 1 and $nFreq$ into a radio channel [13].

In Fig. 2 a TSCH scheduler is depicted. The Enhanced Beacons (EBs) are broadcast packets and, thus, they are transmitted during the contention-based cells, i.e., during the first cell. The other unicast transmissions take place within dedicated cells. As it can be observed, one transmission is allocated per timeslot to each radio link.

B. Blacklisting Techniques

The concept of the blacklisting approach consists of two steps. First, each pair of nodes must identify the radio channels that present poor performance, e.g., low reliability and/or dynamic link qualities [14]. Then, the nodes will block these radio channels so that they are not used for transmissions. More specifically, they will exclude these links from the frequency hopping sequence, i.e., Eq. (1). Thus, all the communications in the network will take place only over the highly reliable radio links. It is straightforward to observe that a large number of blacklisted channels may reduce the network capacity (since a smaller number of channels can be used). On the other hand, a small number of blacklisted channels may result in a high number of retransmissions, with a negative impact on both the reliability and the energy consumption.

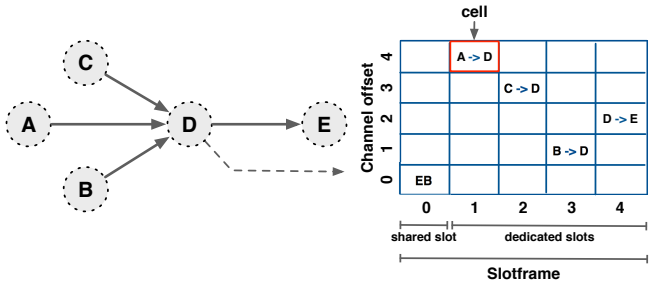

Fig. 2. A TSCH-based scheduler for node D: A $\rightarrow$ D stands for *'A transmits to D'*, while Enhanced Beacon (EB) cells are used for advertisement frames.

A Blacklisting algorithm may be applied either locally or globally in a Low Power and Lossy Network (LLN), with pros and cons for each approach. When it is applied locally, then each pair of nodes may obtain different lists [10]. However, local blacklisting presents a high complexity and, moreover, may introduce collisions when two or more radio links employ the same timeslot, even with different blacklists and channel offsets. On the contrary, when the global approach is employed, then all the nodes in a LLN will have the same list of good radio channels [11]. However, such a solution may be suboptimal since the radio links present different performance depending on their location in the network [7].

III. Local blacklisting issues & analysis

In local blacklisting, each node keeps its own blacklist. This list is exchanged between each communicating pair of nodes (the child and the parent) so that the two nodes retain the same blacklist to communicate properly [10].

Gomes et al. [12] recently presented a localized blacklisting solution where a set of channel offsets is initially assigned to each node. The offsets are used to generate a whitelisted channel using Eq. (1). The radio channel generation is an iterative process where one offset is utilized per time. If no whitelisted channel is generated with the first assigned offset, the second offset is used and so on. Note, that if no whitelisted channel is generated, the node postpones its transmission in the current timeslot, causing delays in the resulting packet delivery. Moreover, packet postponement increases the energy consumption since the receiver switches its radio on even if no packet is sent. Another disadvantage of this approach is that the computation of multiple offsets in a localized manner is a hard task (in [12] this is done centralized). However, the advantage of the method is that the generated channels never overlap with those of their neighboring nodes transmitting at the same time. Hereafter, we present a theoretical analysis of this solution along with an example.

The channel generation process of this local blacklisting approach is illustrated in the example of Fig. 3 for a random ASN value (i.e., $ASN = 50$)[1]. Let us say that three offsets

[1]We use a 0-15 radio channel numbering instead of the default 11-26.

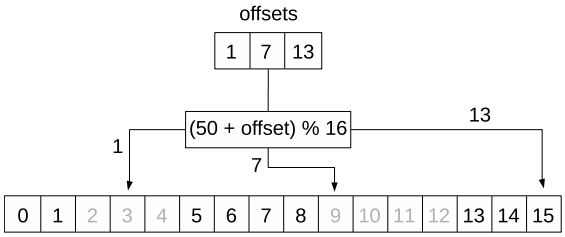

Fig. 3. Radio channel generation process using multiple offsets (channels with gray are blacklisted).

are available (i.e., 1, 7, 13) and channels 2-4 and 9-12 are already blacklisted. Note, that these channels are marked as unavailable so the number of available frequencies (i.e., $nFreq$) of Eq. (1) is still 16. As the picture depicts, the first two offsets generate a channel that is already blacklisted, so a third offset is used to finally get a whitelisted channel.

It is straightforward that the more the channel offsets and the less the blacklisted channels, the higher the probability to generate a whitelisted channel. We denote with $P_{success}$ the probability of "at least one whitelisted channel is generated" given a number of available offsets F and a number of blacklisted channels B. This is the probability of dependent events since for a given ASN each particular channel can be generated only with one offset. Thus, it holds:

$$\begin{aligned} P_{success} &= 1 - P\{\text{no whitelisted channel is generated}\} \\ &= 1 - \prod_{x=1}^{F} \frac{B-x+1}{16-x+1} \end{aligned} \tag{2}$$

Fig. 4 displays $P_{success}$ for different numbers of blacklisted channels and available channel offsets. We can observe that the probability of generating a whitelisted channel using this local blacklisting method is low even with a moderate number of blacklisted channels and available offsets. This behavior could cause severe packet delays in the presence of high interference.

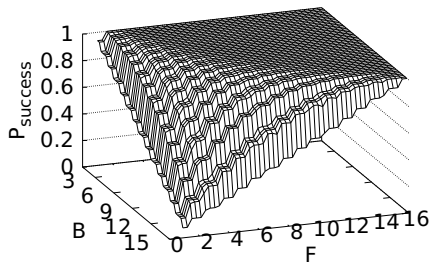

Fig. 4. Probability of generating a whitelisted channel given a number of blacklisted channels (B) and a number of available offsets (F).

Since the number of blacklisted channels depends on external factors, the key point in local blacklisting is how many channel offsets (i.e., F) can be available for the radio channel generation. F is computed during the construction of the data transmissions scheduling and may depend on many parameters, like the number of parallel-neighboring data transmissions in the scheduling, the node density, and the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL)[2] functionality. Next, we present a theoretical analysis of the worst case scenario assuming a uniform node distribution.

The worst case scenario appears when all the neighboring nodes of an arbitrary node which lies close to the center of the terrain transmit or receive data in the same timeslot (see Fig. 5). In this scenario, F depends on the edge chromatic number $\chi(G)$. We denote with $G(V, E)$ the undirected graph with V the set of nodes such that $|V|$ is the number of nodes. E is the set of edges such that every pair of nodes $\{v_1 v_2\}$ $(v_1, v_2 \in V,\ v_1 \neq v_2)$ belongs to E if and only if $\text{dist}(v_1, v_2) \leq r$, where $\text{dist}(\cdot)$ is the Euclidean distance function and r is the nodes' communication range.

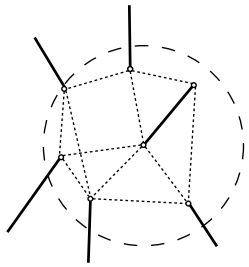

Fig. 5. The worst case scenario: all the neighboring nodes transmit/receive data at the same time (solid lines = active links, dashed lines = physical connections, circle = interference range A).

From Vizing's theorem it is known that $\chi(G) = \Delta$ or $\chi(G) = \Delta + 1$, where Δ is the maximal degree of G. This practically means that F is upper bounded by $\lceil \frac{16}{\Delta} \rceil$. In other words, the maximum value of F per node in G is equal to $\lfloor \frac{16}{\Delta} \rfloor$ or to $\lfloor \frac{16}{\Delta} \rfloor + 1$.

It is straightforward that Δ depends on the node density. Without loss of generality, we assume that we have a square terrain of size $\alpha > r$ and N nodes are randomly deployed in the terrain. We denote with A the interference area defined by the communication range of a node with size $L(A) = \pi r^2$. Assuming a Poisson node distribution process, the mean number of nodes in the region A is λA, where λ is the intensity of the process, which assuming a uniform distribution is $\frac{N}{\alpha^2}$. Thus, the average number of neighbors of a node i is equal to $\lceil \lambda L(A) \rceil - 1$.

$\lambda L(A)$ nodes in A may receive or transmit simultaneously as far as they do not have a double role (receiver/transmitter) and they are assigned on a different channel offset. Since one offset is reserved for the node located at the center of A (communicating with another node in A), there are $\lambda L(A) - 2$ other nodes that can be assigned to a different channel offset (to communicate with nodes outside A). Thus, in the worst case, the total number of offsets F_{max} that can be assigned per node in A is computed as follows:

$$F_{max} = \left\lceil \frac{16}{\lceil \lambda L(A) \rceil - 1} \right\rceil. \tag{3}$$

Fig. 6 illustrates the maximum number of channel offsets for different node populations, a fixed squared terrain of 200×200

[2]The default routing protocol adopted by 6TiSCH Working Group at IETF.

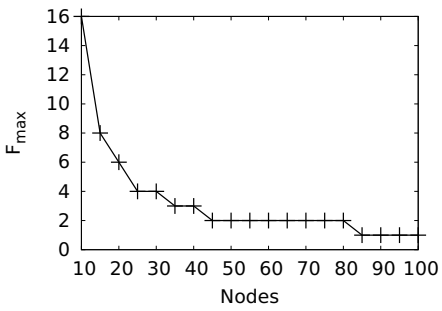

Fig. 6. Maximum number of offsets assigned for different node populations ($\alpha = 200$m, $r = 50$m).

m^2 side and a communication range equal to 50 meters. Note that this is the worst case scenario which appears when all the neighboring nodes receive or transmit data at the same time. Given this scenario, the number of available channel offsets may be extremely limited.

IV. Towards distributed global blacklisting

In this section, we present a distributed global blacklisting method to overcome the limited offset issue of the previous local blacklisting method. The major advantage of our method is that it uses a single offset to generate the radio frequency. Only one offset is required since every time a channel is blacklisted, it is removed from the set of available frequencies and, consequently, $nFreq$ of Eq. (1) is reduced by 1. Thus, the modulo computation will always generate a whitelisted radio channel. This process is depicted in Fig. 7 with only 9 whitelisted channels available. The mapping function returns the 7th element of the list which is radio channel 13.

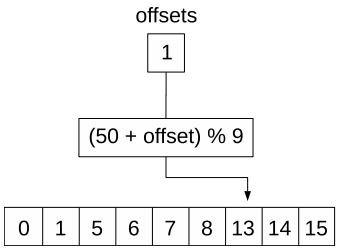

Fig. 7. Channel generation process using a single offset.

However, the single-offset method exhibits two major issues if the nodes are not aware of the blacklisted channels of their neighbors with parallel transmissions. First, there is no guarantee that a generated radio channel will not be the same with any other frequency used by a neighboring pair of nodes and, second, since two neighboring nodes retain different blacklists and whitelists, it is very likely that these two nodes may generate the same channel in future timeslots.

To tackle the previous issues, we need to spread the bad radio channels in the entire network. To do so, every node retains a third list; the list of temporarily *bad* channels. This list contains radio channels that have been detected to have a negative impact on data communications but are not yet permanently blacklisted. Every time a radio channel is moved to this list, it has to be distributed to the whole network so that all the nodes retain the same blacklist in future channel computations. However, another question that arises is *when* a temporarily blacklisted channel should be permanently blacklisted and *when* it will be safe to use the new blacklist.

To solve this new issue, every time a node temporarily blacklists a channel, it associates it with a specific future timing ASN_{BL}. Every node that has this radio channel in its temporary list will permanently blacklist this radio channel at a time that is equal to or later than ASN_{BL} (depending on when it wakes up). The nodes exchange the temporarily blacklisted radio channels every time they communicate with each other by encapsulating this information into the data or the acknowledgement packets without increasing the payload considerably [12]. However, ASN_{BL} must be long enough so that the information can travel to the entire network and every pair of nodes starts using a new blacklist at a proper time.

Apparently, the more often a node communicates with its parent or with its children, the faster a temporarily blacklisted channel is disseminated to the network. For example, assuming that each node participates in the scheduling at least once per slotframe, at least h slotframes will be needed to forward the information even to the most distant nodes. h here is the number of hops between the node which has temporarily blacklisted the channel and its most distant node. h depends on how often each pair of nodes communicates in the scheduling but it also depends on how many times a data packet (or acknowledgement) was successfully delivered to the next (or previous) hop. However, due to the channel hopping mechanism, there is a high probability that a packet that was lost in the previous transmission be successfully delivered in the next slotframe. Moreover, since the same frequency may be used after three hops, it is (usually) safe to start using a new blacklist when the information has been disseminated at least 3 hops away.

The distributed global blacklisting approach solves the limited offsets problem of local blacklisting while it distributes the bad channels to the entire network so that all the nodes retain the same consistent blacklist and generate non-overlapping frequencies. Blacklisted radio channels can be moved back to the whitelisted set after some time, however, this is also an action that must be done simultaneously by all the nodes. The time a channel remains blacklisted can be decided locally by the node which blacklisted this particular channel or it can be empirically predefined (e.g., after some minutes). In the first case, the information needs to be propagated again to the entire network. The second case is simpler but it may cause several transmission failures in case external interferences still exist when the channel is whitelisted (until it is blacklisted again).

V. Evaluation & Discussion of the results

A. Simulation Setup

In this section, we evaluate the local and the global blacklisting schemes presented in the previous sections. We conduct a set of Monte Carlo simulations using the well-known DeTAS scheduling algorithm [15] enhanced with the

blacklisting mechanism. The topologies were generated using a square terrain of $200 \times 200\ m^2$ size, random node positions, and a communication range of $50m$. Each node in the network generates one packet per slotframe. In order to capture the impact of the number of blacklisted channels on the algorithms' performance, we place two IEEE 802.11g access points, i.e., Interference Points (IP), at random positions continuously transmitting data on channels 1 and 6, respectively. Due to the presence of the two IP, several IEEE 802.15.4 channels may overlap with the 802.11 channels. Thus, there is a possibility that packets of the IEEE 802.15.4 network be suppressed by or collide with packets of the external networks. We use a set of empirical values for this probability [3], [4]. These values are displayed on Table I. Finally, we assume that a radio channel is (temporarily) blacklisted if the PDR for this specific channel per link falls bellow 0.9. The value of ASN_{BL} for the global blacklisting solution is set to 5 slotframes.

We vary the number of nodes in the network and we measure the PDR and the total packets delayed within 100 slotframes. We consider that a packet is delayed when it is not successfully delivered to the next hop within the desired timeslot. Each scenario is executed 250 times and the average results as well as the 95% confidence intervals are presented. The local and the global blacklisting approaches are displayed as Local-BL and Global-BL, respectively.

B. Performance Evaluation Results

Fig. 8 depicts the number of packets that were not delivered within the desired interval of 100 slotframes. In this simulation campaign, we capture packets that were lost (a) due to interfering parallel transmissions in the Global-BL case and (b) due to limited available offsets in Local-BL. Packets that were lost due to collisions with the IP are not included in this figure. The results show that Local-BL suffers a higher number of delayed packets due to the increased probability of running out of offsets as more nodes are added in. The validity of this last statement is strengthened by the findings presented in Fig. 9. The average number of offsets assigned per link is measured not to exceed 4, while it trends to decrease as we move to denser scenarios. We can also observe that the number of offsets slightly increases for 90 and 100 nodes which causes a decrease of the delayed packets. On the other hand, the number of blacklisted channels may go up to 8 due to the presence of the two external IP. Thus, according to Eq. (2) there is a probability lower than 0.4 to generate a whitelisted channel for some links.

Fig. 10 depicts in detail the behavior of the average number of blacklisted channels and the packets delayed per slotframe for an example with 100 nodes. Local-BL was only used in this scenario. As the number of slotframes increases, more channels are on average blacklisted. The results show that the number of delayed packets increases as well due to the decreased probability of finding a whitelisted channel.

In Fig. 11, the network reliability is illustrated. We can see that the number of delayed packets has a negative impact on the packet delivery ratio which starts to drop for scenarios with

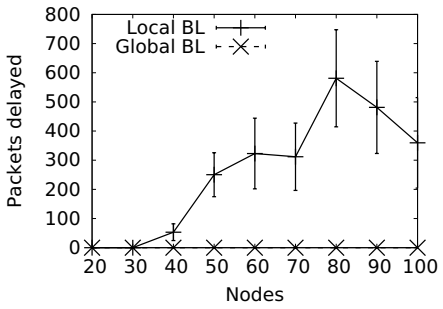

Fig. 8. Total number of packets delayed for different node populations.

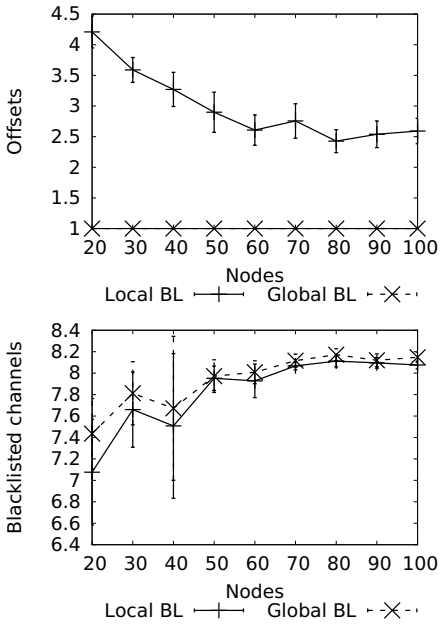

Fig. 9. Average number of available offsets (upper) and maximum number of blacklisted channels for different node populations (lower).

40 or more nodes. On the other hand, the performance of the two approaches is identical for sparser node deployments.

VI. Conclusions & Future work

In this paper, we studied the problem of radio channel blacklisting in IEEE 802.15.4 TSCH networks. We theoretically showed that the current multi-offset local blacklisting method exhibits a major weakness in the presence of high external interference. This weakness may cause packet delays and decreased packet delivery ratio. Simulation results confirmed this issue. To tackle this weakness, we presented a distributed global blacklisting approach using a single-offset technique. The comparison with the previous approach highlighted higher packet delivery ratios with the minimum possible delays. In our future work we want to confirm the findings of the current study using experimentation in real world settings with realistic interference scenarios as well as to assess the performance of the distributed global blacklisting approach with different packet rates and with the use of link quality estimators.

TABLE I
PROBABILITY OF COLLISION BETWEEN IEEE 802.15.4 AND 802.11G CHANNELS.

802.15.4 channels \ 802.11g channels	1	2	3	4	5	6	7	8	9	10	11	12	13
11	0.2	0.05	0	0	0	0	0	0	0	0	0	0	0
12	0.9	0.6	0.05	0	0	0	0	0	0	0	0	0	0
13	0.8	0.9	0.2	0.05	0	0	0	0	0	0	0	0	0
14	0.1	0.9	0.6	0.2	0.05	0	0	0	0	0	0	0	0
15	0	0.2	0.8	0.9	0.2	0.05	0	0	0	0	0	0	0
16	0	0	0.2	0.8	0.9	0.4	0.05	0	0	0	0	0	0
17	0	0	0	0.2	0.8	0.9	0.4	0.05	0	0	0	0	0
18	0	0	0	0	0.1	0.8	0.9	0.4	0.05	0	0	0	0
19	0	0	0	0	0	0.4	0.8	0.9	0.4	0.05	0	0	0
20	0	0	0	0	0	0	0.2	0.8	0.9	0.4	0.05	0	0
21	0	0	0	0	0	0	0	0.2	0.8	0.9	0.2	0.05	0
22	0	0	0	0	0	0	0	0	0.2	0.8	0.9	0.2	0.05
23	0	0	0	0	0	0	0	0	0	0.2	0.8	0.9	0.2
24	0	0	0	0	0	0	0	0	0	0	0.2	0.8	0.9
25	0	0	0	0	0	0	0	0	0	0	0	0.2	0.8
26	0	0	0	0	0	0	0	0	0	0	0	0	0.2

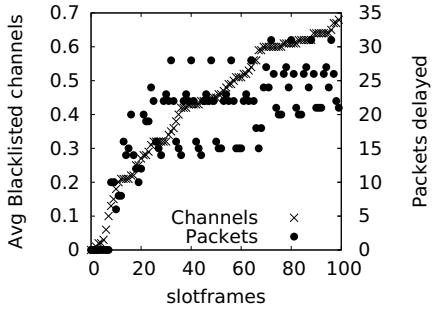

Fig. 10. Average blacklisted channels per node and number of packets delayed per slotframe for a scenario with 100 nodes.

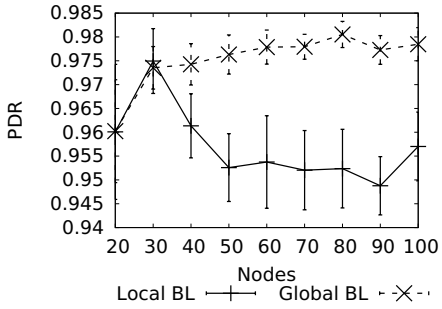

Fig. 11. Packet delivery ratio (PDR) for different node populations.

ACKNOWLEDGEMENTS

This work was carried out within the action "Strengthening Post Doctoral Research" of the "Human Resources Development Program, Education and Lifelong Learning", 2014-2020, which is being implemented from IKY and is co-financed by the European Social Fund – ESF and the Greek government.

It has been also partially supported by the University of Piraeus Research Center and the Greek General Secretariat for Research and Technology under its matching funds programme.

REFERENCES

[1] "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.

[2] A. Hithnawi, H. Shafagh, and S. Duquennoy, "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, 2014, pp. 49–56.

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

[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] L. Tytgat, O. Yaron, S. Pollin, I. Moerman, and P. Demeester, "Analysis and experimental verification of frequency-based interference avoidance mechanisms in ieee 802.15.4," *IEEE/ACM Transactions on Networking*, vol. 23, no. 2, pp. 369–382, April 2015.

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

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

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

[9] W. Specification, "75: Tdma data-link layer," *HART Communication Foundation Std., Rev*, vol. 1, 2008.

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

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

[12] P. H. Gomes, T. Watteyne, and B. Krishnamachari, "MABO-TSCH: Multihop and blacklist-based optimized time synchronized channel hopping," *Transactions on Emerging Telecommunications Technologies*, August 2017.

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

[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] N. Accettura, M. Palattella, G. Boggia, L. Grieco, and M. Dohler, "Decentralized traffic aware scheduling for multi-hop low power lossy networks in the internet of things," in *WoWMoM*. IEEE, 2013, pp. 1–6.