Adaptive Channel Hopping for Wireless Sensor Network

Peng Du
Dept. of Computer Science and Information Systems
Birkbeck, University of London
Marlet Street, London WC1E 7HX
Email: peng@dcs.bbk.ac.uk

Dr. George Roussos
Dept. of Computer Science and Information Systems
Birkbeck, University of London
Marlet Street, London WC1E 7HX
Email: gr@dcs.bbk.ac.uk

***Abstract*—Wireless sensor networks (WSN) are an essential element of the Internet of Things. However, their performance is influenced by many factors such as interference from other co-located wireless communication technologies that are sharing the same spectrum and fading due to environmental factors. Channel hopping is one of several adaptation techniques introduced to mitigate these adverse effects. This paper investigates adaptive channel hopping and the advantages and costs related to augmenting existing WSN systems with this capability. We provide complete design and implementation details on OpenWSN considering specifically the case of IEEE 802.15.4e, and also present the results of our experiments. The main finding of this work is that blacklisting can provide a significant improvement in the performance of channel hopping protocols and thus enhance the overall reliability of WSNs in the presence of interference and fading.**

I. Introduction

Wireless sensor networks (WSN) are increasingly gaining importance and are now recognised as one of the enabling technologies for the Internet of Things [1]. However, they are also facing increasing challenges as the growing interest in wireless communications has led to the emergence of a variety of standards and technologies that utilise the 2.4GHz Industrial Scientific and Medical (ISM) band where WSNs operate [2]. Because the transmission power of wireless sensors is relatively low compared to that of devices such as IEEE 802.11(WLAN) routers, car alarms, wireless video monitors and so forth, coexistence has become a pressing issue [3], [4].

Channel hopping, a technique that periodically changes the operating frequency of the communications channel, is one of the approaches proposed to address the problem. Channel hopping improves the reliability by averaging the risk of being interfered among all available channels [5] and has been adopted by standards including Bluetooth and the forthcoming IEEE 802.15.4e [6], [7].

In [8], blacklisting was proposed as a mechanism that can further improve the performance of channel hopping based on a statistical argument. Blacklisting works by restricting channel hopping to a subset of the spectral space thus avoiding some channels. Although blacklisting has been used in the context of technologies such as [9], no specification of implementation has been provided.

This paper investigates the adaptive channel hopping technique based on a dynamic blacklisting algorithm and the main contributions are threefold. First, an algorithm for adaptive channel hopping is proposed; secondly, the proposal is implemented in the context of a wireless sensor network; and thirdly the experimental results are discussed, demonstrating the enhancement of performance.

The remainder of the paper is structured as follows: section II reviews some of the work regarding channel hopping and blacklisting. The rationale and design for our algorithm are discussed in section III and implementation details are provided in section IV. After a brief description of experimental settings in section V, results and findings are subsequently presented and analysed in Section VI. Finally conclusions are drawn in Section VII.

II. Related Work

The channel hopping technique has been embraced by many technologies and standards. For instance, Bluetooth [6] utilises 79 1-MHz channels in the 2.4GHz band and devices change their operating channels in a certain pattern to improve the coexistence with, for example, IEEE 802.11.

Another example is WirelessHART [9], an open-standard technology for IEEE 802.15.4 compatible sensors. WirelessHART works on top of Time Synchronized Mesh Protocol (TSMP) [5] which divides time space into an infinite number of discrete slots. An absolute slot number (ASN) records the count of elapsed timeslots and is sychronised in all nodes. Operating channels are calculated using ASN, therefore communications within each timeslot take place in pseudo-randomly chosen channels. Such a feature reduces the impacts of interference as well as multi-path fading [8].

Channel hopping is currently being drafted in IEEE 802.15.4e Task Group [7] as an enhancement to the existing IEEE 802.15.4 standard. Similar to WirelessHART, IEEE 802.15.4e is TSMP-based. Time is viewed as a series of

consecutive superframes, each consisting of a configurable number of timeslots. Synchronisation is achieved by exchanging ASN-inserted advertisement (ADV) packets in dedicated "ADV slots" of each superframe.

Furthermore, both Bluetooth and WirelessHART support the removal of certain channels from the channel hopping sequence, known as adaptive frequency hopping (AFH) [6] and Blacklisting [10], respectively, but provide no standardised implementations. To investigate the performance of blacklisting, [8] replays previously gathered channel hopping data traces with different blacklist sizes applied and finds an improved packet delivery rate (PDR). However the work is purely statistical and suggests no algorithm for blacklisting.

An essential requirement for adaptive channel hopping is to identify the undesirable channels to be blacklisted. [11] demonstrates using Packet Delivery Ratio (PDR) as the metric for channel quality. Nevertheless, a relatively long sampling period (15 minutes) is required for each channel which makes this method inefficient in capturing changes in channel situations. Spectrum sensing [12], [13], on the other hand, provides an alternative approach to channel condition assessment and is explored in following sections.

Making adjustments on-the-fly in accord with the blacklisting decisions is equally important for adaptive channel hopping. Cognitive Radio (CR) technology [14] enables a system to reconfigure itself by interacting with the environment [15] and is thus a suitable tool for this work.

III. Adaptive Channel Hopping

In this paper we defined adaptive channel hopping as the blacklisting-enabled channel hopping technique as opposed to the blind channel hopping of the current IEEE 802.15.4e.

A. Rationale

The wireless spectrum is not uniformly utilised and consequently specific frequency ranges suffer disproportionately from interference [16]. Using such "crowded" frequencies degrades communication performances and should be avoided. Adaptive channel hopping is able to achieve this aim by blacklisting i.e. dynamically adjusting the behaviour of channel hopping so that crowded channels are excluded from the sequence. Strategies for the effective selection of blacklisted channels are a critical ingredient of this technique.

Packet Delivery Ratio (PDR) is a possible indicator of channel quality [11], [17] that could be used for such a purpose. For example, a channel can be classified as "lossy" once the PDR falls below a pre-defined threshold and later blacklisted. However, PDR as a metric has an inherent disadvantage since it only provides meaningful indication after a sufficient number of packets have been sent in the channel that is being probed. As a result systems might not be able to update the blacklist promptly.

Alternatively, adaptive channel hopping uses noise floor listening for selecting channels to blacklist. In this paper noise floor is defined as the spectrum energy level that reflects the intensity of utilisation. Because wireless sensor networks use the license-free 2.4GHz ISM band where multiple types of devices operate [18], narrow-band interference is the main factor in the performance. By identifying and blacklisting heavily utilised channels the risk of interference can be mitigated.

B. Algorithm

Noise floor listening is conducted by accessing the Received Signal Strength Indicator (RSSI) from the radio chipset. RSSI values exhibit a very linear function of input power [19], which makes it a suitable metric.

Communications are periodically suspended to create "quiet" periods to acquire valid noise floor readings. A Blacklisting Manager (BLM) component is implemented in each node. It calculates the mean RSSI of a different channel during each quiet period and counts the number of the results that exceed a threshold of -87dBm, which is based on the findings in [20]. These counts are defined as the noise level indicators (NLI) of each channel.

A blacklist has the form of a 16-bit mask and each bit corresponds to a channel. During each periodic blacklist updating, the associated bit of the channel with the highest NLI is set to false by BLM. Every time a node needs to hop to a new channel, its BLM first checks the channel number against the mask. If it is not blacklisted then operations continue as normal; when the channel turns out blacklisted, BLM randomly generates a new channel number and repeats the process until an allowed channel is acquired.

IV. Implementation

A. OpenWSN

The open source implementation of IEEE 802.15.4e by Berkeley's OpenWSN project [21] is used as the basis for this work. The very first slot of every superframe is reserved as the "ADV slot". Once synchronised, nodes communicate in channels computed with the following equation:

$$Channel = (ASN + ChannelOffset)\%16 + 11 \qquad (1)$$

A superframe is configured to contain 11 timeslots and "ChannelOffset" is given a constant of zero. As equation (1) suggests, all 16 channels are used indiscriminately. Thus this type of channel hopping technique is referred to as "blind".

B. Blacklisting

Each superframe has two slots dedicated to noise floor listening. Communications are suspended in these timeslots and noise floors of channels calculated with equation (1) are probed. It can be inferred from the aforementioned OpenWSN

TABLE I
BLACKLIST SIZE FOR 5 EXPERIMENTS

Experiment	a	b	c	d	e
Size of blacklist	0	3	6	9	Unrestricted

parameters and equation that a scan of all 16 channels takes 8 superframes (16 noise floor timeslots), approximately 1.76 seconds with a pre-defined slot time of 20ms. Once per 128 superframes BLM blacklists the channel with the highest NLI and channel masks are into ADV packets by all nodes so that the blacklist are synchronised simultaneously with ASN.

Besides the NLI, a record of noise floors is kept by BLM using equation (2) to provide additional information for experiments in next section.

$$NF[c]_k = \alpha NF[c]_{k-1} + (1-\alpha)RSSI[c]_k \qquad (2)$$

Where $k \in \{2, 3...\infty\}$, $c \in \{1, 2...16\}$, $\alpha \in \{0, 1\}$ and $NF[c]_1 = RSSI[c]_1$.

$NF[c]_k$ is the record of channel *c* after *k* times of noise floor listening. $NF[c]_1$ is assigned the first average RSSI acquired $RSSI[c]_1$. Values afterwards are weighed mean of historical records and most recent RSSI readings, subject to coefficient α. α is currently set to 0.5, which gives equal weight to the most recent reading and previous records.

V. EXPERIMENTS

Our experiments make use of *N* TMote Sky sensors [22] equipped with identical adaptive channel hopping functionality. One of the nodes is connected to an IPv6 gateway router and appointed as the coordinator.

Experiments were conducted in an open office environment, where typically an excess of 10 WLANs and several Bluetooth devices are in operation. Each node is configured to send 300 packets to the coordinator at 0.5Hz. Experiments were carried out with different blacklist sizes shown in Table I from column (a) to (e).

A zero-sized blacklist for (a) indicates that blind channel hopping is used because no channel can be blacklisted. In contrast, any number of channels can be blacklisted in (e) as long as its associated RSSI record calculated with equation(2) is above the threshold used to compute NFI. Experiments with configuration (a)-(e) were repeated 4 times respectively so a total of 20 tests took place.

VI. EXPERIMENTAL RESULTS

The solid line in Figure 1 represents the average length of time (seconds) used to transmit all 300 packets in experiment (a)-(e) respectively. Values are averaged over 4 instances of each experiment and marked beside the filled diamonds.

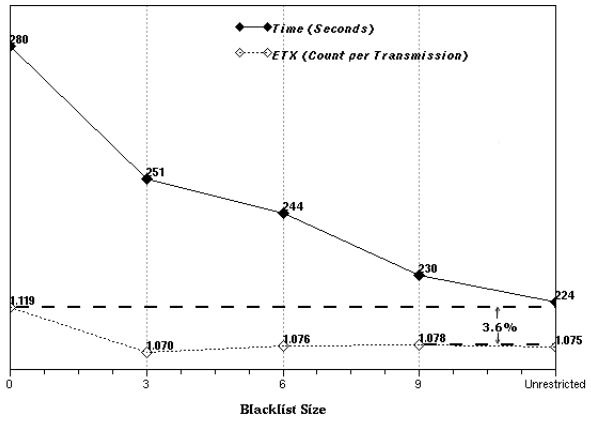


Fig. 1. The average length of time required to complete the transmissions of all packets (solid line with filled diamonds) tends to be shorter when blacklisting (non-zero blacklist size) is used . Blacklisting also makes average Expected Transmission Count (dashed line with hollow diamonds) at least 3.6% lower, indicating a better chance of successful transmissions.

It is observed that transmissions finish more quickly when blacklisting is enabled. This is because transmissions using IEEE 802.15.4e are paused if senders do not receive valid advertisement (ADV) packets as expected and become out of sync. The fact that experiment (b)-(e) spent less time than (a) to complete implies that adaptive channel hopping is able to mitigate the losses of ADV packets, which in turn reduces time wasted in awaiting ADV packets to resynchronise and makes transmissions more efficient.

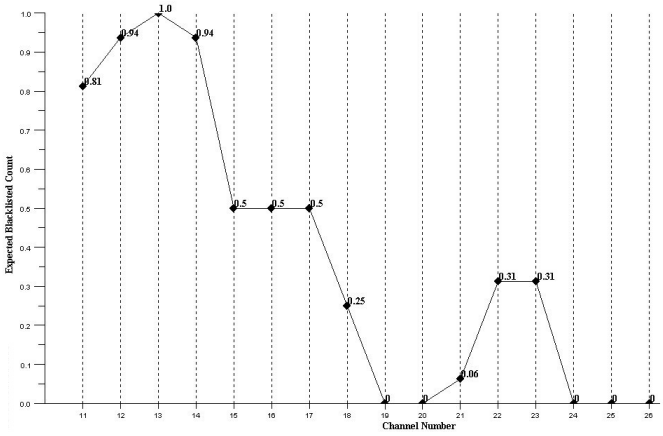
The hollow diamonds on the dashed line in Figure 1 mark the average Expected Transmission Count (ETX), defined as $\frac{1}{PDR}$ [23], of all experiments. Since Packet Delivery Ratio (PDR) represents the probability of a transmission being successful, ETX is the average number of attempts a sender has to make for a packet to be correctly received [8]. The figure shows that the average ETXs are at least 3.6% lower when backlisting is enabled, demonstrating that adaptive channel hopping improves the chances of successful transmissions by avoiding noisy channels.

Whilst Figure 1 visualises the enhanced performance of adaptive channel hopping, the correctness of the blacklisting Manager (BLM) is verified in Figure 2.

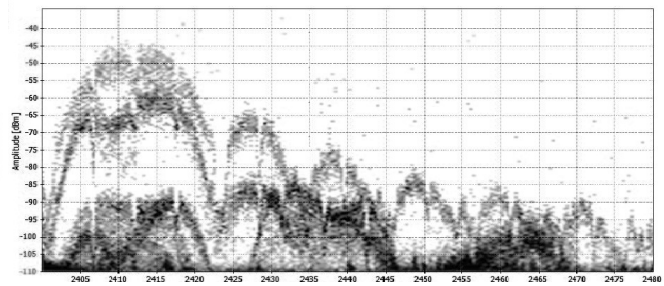
Expected Blacklisted Count (EBC) is introduced as a metric for each channel in Figure 2(a).

$$EBC[c] = \frac{\textit{Times of channel c being blacklisted}}{\textit{Total number of experiments}} \qquad c \in \{1, 2...16\} \qquad (3)$$

According to equation (3), $EBC[c]$ indicates how often channel c is blacklisted by BLM. Figure 2(a) shows channel $\{11$ - $14\}$ are the most frequently blacklisted whilst $\{24$ -



(a)



(b)

Fig. 2. (a) The Expected Blacklisted Count (EBC) of all 16 channels (b) Noise floor from 2405 (channel 11) to 2480MHz (channel 26) captured with Wi-Spy.

26} are never disallowed.

Figure 2(b) illustrates the distribution of channel energy level captured with Wi-Spy spectrum analyser [24] during the period of experiments. It is seen that channel {11 - 14} (2405 - 2420MHz) are the most noisy frequencies and channel {24 - 26} (2470 - 2480MHz) are relatively quiet. This is consistent with the findings in Figure 2(a) and proves that the BLM is able to correctly estimate the noise floors of the channels.

VII. Conclusion

Channel hopping has already been proved effective in improving packet delivery ratio (PDR) in the presence of interference and multi-path fading [8], [25]. By using blacklisting it is possible to further improve the effectiveness of this approach by avoiding those channels where packets are most likely to be lost. In this paper, an algorithm for adaptive channel hopping is described and implemented. By assessing the channel noise floor, heavily utilised channels can be identified and blacklisted. Preliminary experimental evidence suggests adaptive channel hopping's advantage over blind channel hopping in terms of packet delivery ratio and efficiency. Moreover the mechanism for channel quality evaluation is verified with the off-the-shelf spectrum analyser.

References

[1] L. Benini *et al.*, "Wireless sensor networks: Enabling technology for ambient intelligence," *Microelectron. J.*, vol. 37, pp. 1639–1649, December 2006.

[2] S. Pollin *et al.*, "Distributed cognitive coexistence of 802.15.4 with 802.11," in *1st Int. Conf. Cognitive Radio Oriented Wireless Networks and Comm.*, 2006.

[3] H. Khaleel *et al.*, "Impact of Wi-Fi traffic on the IEEE 802.15.4 channels occupation in indoor environments," in *Int. Conf. Electromagnetics in Advanced Applications, 2009. ICEAA '09.*, 2009, pp. 1042 – 1045.

[4] C. M. D. Dominicis *et al.*, "Investigating WirelessHART coexistence issues through a specifically designed simulator," in *Instrumentation and Measurement Technol. Conf. 2009 IEEE*. IEEE, 2009, pp. 1085–1090.

[5] K. S. J. Pister and L. Doherty, "TSMP: Time Synchronized Mesh Protocol," in *Parallel and Distributed Computing Systems*, 2008.

[6] *Bluetooth Core Specifications version 4.0*, SIG Bluetooth Std.

[7] IEEE 802.15 WPA Task Group 4e (tg4e) website. [Online]. Available: http://www.ieee802.org/15/pub/TG4e.html

[8] T. Watteyne *et al.*, "Reliability through frequency diversity: why channel hopping makes sense," in *Proc. 6th ACM Symp. Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*. ACM, 2009, pp. 116–123.

[9] "WirelessHART technical data sheet."

[10] Co-existence of WirelessHART with other wireless technologies. [Online]. Available: http://www.hartcomm.org/protocol/training/resources/wiHART_resources/

[11] B. Kerkez *et al.*, "Feasibility analysis of controller design for adaptive channel hopping," in *Proc. 4th Int. ICST Conf. Performance Evaluation Methodologies and Tools*. ICST, 2009, pp. 76:1–76:6.

[12] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, pp. 201–220, 2005.

[13] I. F. Akyildiz *et al.*, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, 2006.

[14] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Commun. Mag.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[15] I. F. Akyildiz *et al.*, "Crahns: Cognitive radio ad hoc networks," *Ad Hoc Netw.*, vol. 7, pp. 810–836, July 2009.

[16] Y. Liu, "Performance improvement of wireless communications using frequency hopping spread spectrum," *Int. J. Commun., Network and System Sci.*, vol. 3, pp. 805–810, Oct. 2010.

[17] R. Tomasi *et al.*, "Frequency agility in IPv6-based wireless personal area networks (6LoWPAN)," in *WWIC'10*, 2010, pp. 146–157.

[18] C. T. Ee, "Interference avoidance in wireless multihop networks," poster session presented at the 2nd Annu. IEEE Commun. Soc. Conf. Sensor and Ad Hoc Commun. and Networks, 2005.

[19] "Chipcon CC2420 datasheet." [Online]. Available: http://inst.eecs.berkeley.edu/~cs150/Documents/CC2420.pdf

[20] K. Srinivasan and P. Levis, "RSSI is under appreciated," in *Proc. 3rd Workshop on Embedded Networked Sensors (EmNets*, 2006.

[21] Berkeley's openwsn. [Online]. Available: http://openwsn.berkeley.edu

[22] "TMote Sky datasheet." [Online]. Available: http://www.bandwavetech.com/download/tmote-sky-datasheet.pdf

[23] D. S. J. D. Couto, "High-throughput routing for multi-hop wireless networks," Ph.D. dissertation, MIT, June 2004.

[24] Wi-Spy. [Online]. Available: http://www.metageek.net/products/wi-spy/

[25] N. Golmie *et al.*, "Bluetooth adaptive frequency hopping and scheduling," in *Proc. IEEE conf. Military Commun.* Washington, DC, USA: IEEE Computer Society, 2003, pp. 1138–1142.