Design and implementation of a transmission protection protocol to improve the performance of wireless sensor networks in hybrid networks

Jang-Ping Sheu*, Shu-Hsun Wu, Chuang Ma and Wei-Kai Hu

Department of Computer Science,
National Tsing Hua University,
Hsinchu, 30013, Taiwan
E-mail: sheujp@cs.nthu.edu.tw
E-mail: s9962556@m99.nthu.edu.tw
E-mail: machuang@mx.nthu.edu.tw
E-mail: huwk@mx.nthu.edu.tw
*Corresponding author

Abstract: In hybrid networks, the devices of Wireless Local Area Networks (WLANs) and Wireless Sensor Networks (WSNs) will interfere with each other when working in a same area because they use the same band, 2.4 GHz. With the greater transmission power and more aggressive channel access time resolution, WLANs often affect the communication of WSNs severely. To eliminate this kind of interference effect, we design protection nodes and propose a transmission protection protocol, WSNs Transmission Protection Protocol (WTPP), to improve the transmission performances of WSNs in hybrid networks. The protection nodes can emit protection signal periodically to block the traffic of WLANs and permit the transmission of WSNs. We implement WTPP in a hybrid network testbed to prove its feasibility. Comparing with legacy ZigBee, the experimental results show that WTPP can improve the packet delivery ratio of WSNs efficiently under the interference of WLANs. When WSNs work on low duty cycle, the throughput degradation of WLANs is less than 6%.

Keywords: hybrid networks; transmission protection; WLANs; wireless local area networks; WSNs; wireless sensor networks.

Reference to this paper should be made as follows: Sheu, J-P., Wu, S-H., Ma, C. and Hu, W-K. (2014) 'Design and implementation of a transmission protection protocol to improve the performance of wireless sensor networks in hybrid networks', *Int. J. Ad Hoc and Ubiquitous Computing*, Vol. 17, No. 4, pp.244–253.

Biographical notes: Jang-Ping Sheu is currently a Chair Professor of the Department of Computer Science, National Tsing Hua University. His current research interests include wireless sensor networks, cognitive networks and cloud computing. He is an IEEE Fellow.

Shu-Hsun Wu received his Master's degree in Computer Science from National Tsing Hua University, Taiwan, in 2012. His research interests include wireless sensor networks and wireless local area networks.

Chuang Ma received his BS in Automatic Control from Harbin University of Science and Technology, China, in 1997, MS in Software Engineering from Harbin Institute of Technology, China, in 2004 and PhD in Computer Architecture from Harbin Institute of Technology, China, in 2011. He is a postdoctoral Fellow of the Computer and Communication Research Center, National Tsing Hua University, Taiwan. His current research interests include wireless communications and mobile computing. He is a member of the IEEE and ACM.

Wei-Kai Hu received his BS in Computer Science and Information Engineering from Tunghai University, Taichung, Taiwan, in 2001 and PhD in Computer Science and Information Engineering from National Central University, Taiwan, in 2010. Now, he works as a Postdoctoral Researcher in National Tsing Hua University. His research interests include wireless sensor networks, ad hoc networks and VANETs.

1 Introduction

Nowadays, it is common that multiple heterogeneous networks coexist in the same area of application scenarios, such as hospitals, schools and factories. For example, in a hospital, Access Points (APs) provide access to the internet for hand-held devices or laptops in WLANs where WSNs mobile nodes monitor and report patients' physical conditions to the nursing centre periodically in the same time (Oliveira et al., 2012). Sharing spectrum in hybrid networks will increase undoubtedly communication spectrum utilisation. However, it will also bring brand-new challenges when two networks coexist together. For example, the performance of WSNs will degrade dramatically when the nodes of WSNs encounter in the WLANs environment with medium to high traffic. The packet delivery ratio of WSNs decreases fiercely when the traffic in WLANs increases (Guo et al., 2011). The coexistence problem between WSNs and WLANs is reported in previous studies. By an indoor testbed with randomly deployed nodes, the authors in Gummadi et al. (2009) reported that the packet loss rate of WSN exceeds 20% under WLAN interference, and it will even exceed 85% when the nodes of WSNs face extremely heavy WLAN interference. In Liang et al. (2010), a 90-node WSN was put in a lecture hall for building energy management application, and an enterprise WLAN was also deployed in the same space. During the peak period of the usage of WLAN, it was observed that nearly half of the WSN nodes suffered from connection loss and their communications became unreachable. Similar results are reported in Hauer et al. (2009), Huang et al. (2010) and Liu et al. (2010); they all discovered the performances of WSNs severely degraded when there are medium to high traffics of WLANs.

In many applications, this kind of problems is solved by packet acknowledgement and retransmission mechanism traditionally (Crossbow Technology Inc., 2004). Unfortunately, it did not afford good results because it will lead to more excessive retransmission, less power efficiency and longer end-to-end delay when nodes of WSNs face heavy WLAN interference. Thus, most of the previous studies focused on interference avoidance by allocating the channels for WSNs and WLANs without overlapping so they will not affect each other. In interference avoidance approaches, WSNs nodes detect and measure the level of interferences, which are caused by the signal of WLANs. Upon the interference becoming intolerable, the WSNs will be switched to another clean channel by dynamic channel allocation in centralised decision mechanism. However, the dynamic channel allocation faces two major challenges:

- It is hard to handle with the situation with burst traffics in WLANs. The response time from detecting interference to switching channel might be too long for burst interference, thus it will degrade throughput and prolong end-to-end delay.
- It is difficult to ensure the control packets for activating channel switching can be received by all nodes in entire WSNs under an extreme noisy environment.

We propose a WTPP to alleviate the interference in the overlapping frequency channels between WSNs and WLANs. Our protocol uses protection nodes, which will synchronise to the working schedule of WSNs by overhearing the beacon packets in WSNs, to protect data transmissions in WSNs. Protection nodes have greater transmission power than common WSNs nodes and emit protection signal concurrently during the data transmissions in WSNs. The protection signal can strengthen the signal presence of WSNs against WLANs, and defer the transmissions in WLANs based on the CSMA-style spectrum protocol in wireless networks. Also, the protection signal will only affect the WLANs channels that overlap with the channel of protection signal, so that we can protect the data transmissions in WSNs from being interfered by the traffics in WLANs, without impacting to the communications of WLANs on other channels.

The rest of the paper is organised as follows. Section 2 describes related work. Our proposed protocol is presented in Section 3. The implementation details are described in Section 4, and the experimental results are shown in Section 5. In Section 6, we conclude this paper.

2 Related work

To make the efficient coexistence between WLANs and WSNs possible, there are a lot of researches focusing on avoiding or solving the interferences of heterogeneous wireless networks. A straightforward way is to try to allocate the communications of WSN nodes to the channels that are not or less used by WLAN devices at the beginning. However, this is nearly infeasible in reality, because the cost will be very high if we change the channels of WSNs; moreover, the frequency of switching will increase when new WLAN devices are deployed and occupy switched channels. On the Industrial, Scientific and Medical (ISM) band, the number of orthogonal 802.11 channels is limited, and it almost impossible to find a clean 802.15.4 channel for WSNs nodes in a densely deployed WLAN environment.

As alternative methods, channel-hopping mechanism was applied in heterogeneous networks. In a channel-hopping mechanism, WSNs nodes will switch to a less-effected channel when they face interference caused by the traffic of WLANs. However, it is not easy to implement because of restricted requirements of environment. In contrast, another method called non-channel-hopping mechanism was proposed; it assumes that WSNs are put in a densely deployed WLANs environment and there are no clean channels for WSNs. We will discuss these two kinds of mechanisms in detail.

2.1 Channel-hopping mechanisms

In Won et al. (2009), the authors use Received Signal Strength Indicator (RSSI) to detect interference. If the RSSI indication of a node is greater than a threshold in a certain channel, the node will determine that the channel is occupied. And, if most of the nodes' RSSI indications indicate that their channels are occupied, channel interference is recognised. To get rid of the interference, WSNs nodes will adaptively switch to other idle channels. Nevertheless, the switches cannot be applied under heavy traffic of WLANs, because it cannot ensure the successful delivery of channel-switching control packets in strong communication conflictions of WSNs.

The authors in Musåloiu-E. and Terzis (2008) proposed an interference estimator that can be implemented on resource-constrained sensor nodes. In the first phase, each of the nodes on the multi-hop path except the source node and the sink node independently senses the radio-frequency spectrum and chooses radio channel with the least noise. In the second phase, these nodes vote and select a common channel with the least noisy and switch to the agreed channel to transfer data. Although it can find an optimal channel for transmission in the whole path, it will incur long blackout time owing to channel scanning and re-allocation. The cost is very high when the size of network is big. Besides, it cannot ensure that control packets for switching can be received by every node on the path in heavy interference.

2.2 Non-channel-hopping mechanisms

In Huang et al. (2010), the authors proposed WhIte Space-aware framE adaptation (WISE) for WSNs, which predicts the length of white space in WLANs according to the estimation of the idle interval among the traffics in WLANs and intelligently adjusts frame size to maximise the throughput of WSNs. However, WISE needs to suspend the transmission of WSNs for every burst traffic of WLANs, so that it is unsuitable for TDMA data transmissions and delay-sensitive wireless applications.

In Gummadi et al. (2009), the authors proposed a mechanism called Metronome to deal with heterogeneous wireless networks coexistence. In Metronome, the monitors are deployed in the interference area. The monitors continuously sample the energy across the band of interest, and periodically send the information to the central coordinator. On the basis of the information, the central coordinator can calculate the interference contributions of each transmitter and determine the best transmission power and channel setting for transmitters of both WSNs and WLANs. The central coordinator then sends the settings parameters to the transmitters, which can be used to modify their behaviour accordingly. However, this approach is only suitable to static networks without burst traffics, and it requires the ability to control every wireless device in heterogeneous networks, which is hard to achieve in the real application environment.

An alternative way, called BuzzBuzz (Liang et al., 2010), argued that the conflicts occur most likely in the front part of WSNs' packets when WLANs and WSNs devices can detect each other. The distance of recognition between WLANs devices and WSNs nodes is usually less than 2 m. When the mobile nodes begin to be recognised by other nodes, BuzzBuzz will substantially increase the packet delivery ratio of WSNs by using multiple headers against the interference. BuzzBuzz uses Forward Error Correction (FEC) and Automatically Repeat re-Quest (ARQ) when the WLANs devices are too far from WSNs devices to detect the ongoing transmissions of WSNs. However, hop-by-hop FEC check will add inevitable end-to-end delay. Besides, ARQ will cause excessive retransmissions under very noisy environment, which lead to non-efficient power consumption.

A new mechanism was proposed in Zhang and Shin (2011), which is called by Cooperative Busy Tone (CBT). Instead of reallocating channel or altering default settings, it exploits the inherent cooperation in WSNs nodes to harmonise their coexistence with WLANs. It employs a separate device to act as a signaller to send carrier signal when the nodes of WSNs transfer data in interference environment of WLANs. Upon receiving a control packet of WSNs, the signaller will send carrier signal immediately. The carrier signal will enhance the visibility of WSNs to WLANs devices by making WLANs transmissions backoff for transmission of WSNs nodes. Experimental results showed that it can greatly increase the performance of WSNs under severe interference. However, it has three shortcomings.

- To get enough power of carrier signal, it uses a universal software radio peripheral device, GNURadio/USRP2 software radio platform, as signaller. GNURadio/USRP2 does not yet support delay-sensitive MAC operations, so the switching time between sending and reception is too long to protect the ongoing WSN transmissions.
- CBT only supports one-hop transmission, whereas most of the current WSNs applications work in multi-hop transmission.
- Heavy WLANs traffic (such as 16 Mbps or above) will cause high loss rate of control packets in WSNs, which will inevitably decrease the performance of CBT.

3 WSNs Transmission Protection Protocol

To effectively mitigating the interference from WLANs, we will analyse the causes of the conflicting existence firstly.

3.1 The disadvantages of WSNs in hybrid networks

The following are the two main reasons of communication interference of WSNs from WLANs.

3.1.1 Lower transmission powers of WSNs

The transmission power of WSNs nodes is from −25 dBm to 0 dBm (IEEE 802.15 Working Group, 2003), and the transmission power of WLANs devices is from 15 dBm to 20 dBm (IEEE 802.11 Working Group, 2009). The advantage of WLANs' greater transmission power makes it much easier to occupy the frequency band than WSNs and results in degradation of performances in WSNs. When the distance between WSNs nodes and WLANs devices is more than 2 m, the signal sent by WSNs nodes may not be effectively detected by WLANs devices. However, the signal sent by WLANs devices is strong enough to make the WSNs nodes backoff. In the worst case, after five unsuccessful consecutive attempts, WSNs nodes will drop the transmitting packet and try to retransmit the packet in link layer again.

3.1.2 Lower time resolutions of WSNs

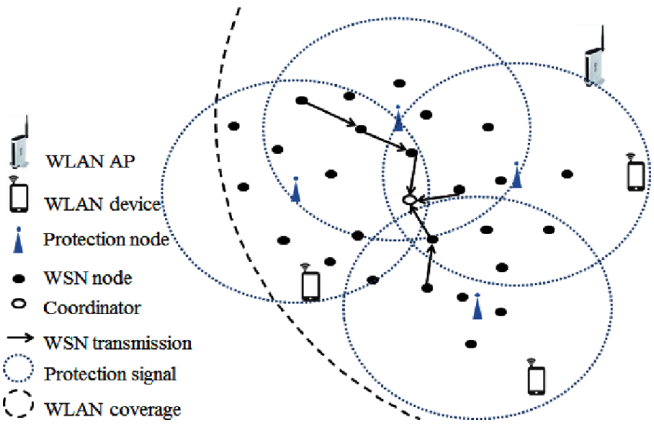
The priority of transmission in WSNs may easily be pre-empted by the traffics in WLANs because of the lower time resolutions of WSNs nodes. For instance, WSNs take 128 µs to perform a Clear Channel Assessment (CCA) operation (IEEE 802.15 Working Group, 2003) whereas WLANs only take 15 µs in 802.11 b/g and 4 µs in 802.11n (IEEE 802.11 Working Group, 2009). A backoff time slot of WSNs is 320 µs and it must wait for an idle channel by two slots before sending data. In contrast, the backoff time slot in WLANs is only 20 µs in 802.11b and 9 µs in 802.11a/g/n. If the CCA operation declares that a channel is busy, WSNs nodes will resume the backoff and wait for the next-round CCA operation until aborting after five consecutive unsuccessful attempts. However, when a WLANs device senses a busy channel, it will persist in channel sensing until it finds an idle slot for transmission. As a result, the time resolution of WLANs is higher and more aggressive than that of WSNs. With much shorter backoff slot and CCA operation time, WLANs devices can perform the whole backoff process and start data transmission even within the time range of data transmission procedure in WSNs. Furthermore, with the more aggressive time resolution, a WLAN device can easily occupy the frequency band whenever it needs for transmissions.

To solve communication interference problems for WSNs from their above-mentioned disadvantages, our protocol will use protection nodes to emit protection signals to make WLANs devices backoff simultaneously with data transmissions in WSNs, to enhance the visibility of WSNs nodes with lower transmission power against WLANs devices. To alleviate the lower efficiency from the lower time resolution of WSNs, the period of protection signal is designed as a long enough time interval to cover the data packets period, the switching time and the corresponding ACK packets period of WSNs. Moreover, the protection signal will send earlier than the beginning of data transmission to prevent potential WLANs pre-emptions.

3.2 The design of WTPP

In WTPP, we use protection nodes to protect the data transmissions in WSNs. The transmission power of protection nodes is big enough to compete with WLANs devices. Each protection node is equipped with two antennas, while one antenna sends out the protection signal, and the other listens to the beacon packets sent from WSNs nodes. Figure 1 illustrates the working scenario of WTPP.

Figure 1 An illustration of the working scenario of WTPP (see online version for colours)



In Figure 1, there is a coordinator node in WSN, which is in charge of coordinating the communications of WSN. Protection nodes are uniformly distributed in the WSN, and each WSN node is covered by one protection node at least. Coordinator broadcasts beacon packets periodically to distribute the working schedule to WSN nodes. WSN nodes can communicate with each other in their active periods and turn into sleeping mode in their inactive periods. By overhearing the beacon packets, protection nodes can obtain the working schedule and synchronise with it. Since protection nodes know when the next WSN active period come and how long it will be, they can emit protection signal simultaneously with the data transmissions in WSN. Under the protection, WSN nodes can transmit packets without being interrupted by the traffic in WLAN. At the same time, the WLAN devices can sense WSN transmission indirectly by detecting the protection signal from protection nodes.

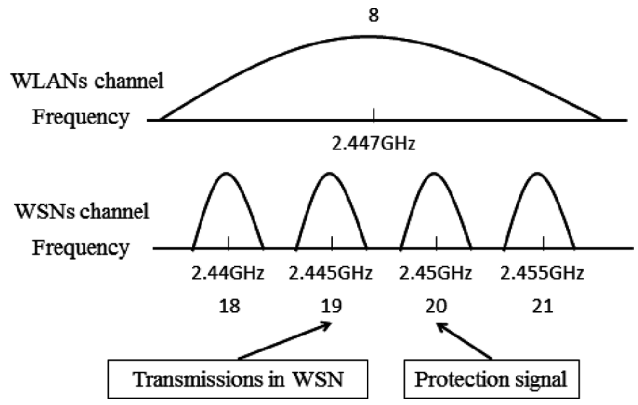
The protection signal will only affect certain WLANs channels that are overlapping with the channel of protection signal. In another word, the communication of WLANs that use other channels will not be interrupted by the protection signals. Moreover, the protection signals will last long enough to cover all data transmissions in one round communication of WSNs and prevent the data transmissions failure from being pre-empted by the traffics in WLANs. To protect efficiently the data transmissions in WSNs, protection nodes must be able to emit protection signals at the right time without interrupting the ongoing data transmissions in WSNs. So in WTPP, we use a protection signal channel selection mechanism and protection scheduler to achieve the goal.

3.2.1 Protection signal channel selection

In WTPP, we leverage the inherent spectrum feature of WSNs and WLANs so that the protection signals will not interrupt the ongoing or forthcoming data transmissions in WSNs. In the 2.4 GHz spectrum, the width of each WSNs channel is 4 MHz and the ith channel is centred at 2.405 GHz + 0.005(i-11)GHz, $i \in [11, 26]$, with 1 MHz guard band between adjacent channels (IEEE 802.15 Working Group, 2003). On contrast, the width of each WLANs channel is 20 MHz and the jth channel is centred at 2.407 GHz + 0.005j GHz, $j \in [1, 11]$. As a result, adjacent channels are partially overlapping with each other (IEEE 802.11 Working Group, 2009) and each WLANs channel overlaps with four WSNs channels. The protection nodes will use one adjacent channel in WSNs to emit the protection signal. Because the adjacent WSNs channels are orthogonal, the protection signal will not interfere with the ongoing transmissions in WSN. However, the protection signal still will overlap with the WLANs channels being currently used, hence it will make the WLANs devices be aware of the existence of the data transmissions in the WSN and defer the upcoming traffics.

An example is shown in Figure 2. We assume the ongoing data transmissions in WSN are on channel 19 under the interference of WLAN's channel 8. To protect the desired data transmissions effectively in WSN, protection nodes will use channel 20 to emit the protection signal. Since channels 19 and 20 are orthogonal to each other, the protection signal will not conflict with the data transmissions in channel 19. However, channel 20 still overlaps with WLAN's channel 8, so that the protection signal can still make effectively the traffic of the WLAN backoff by its big enough transmission power.

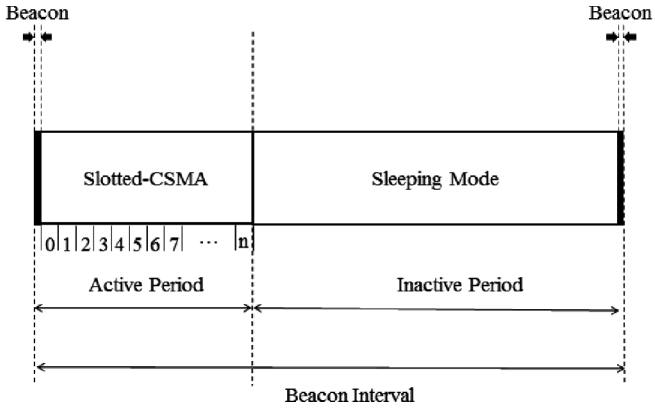
Figure 2 Protection node emit protection signal on an adjacent channel to avoid interfering the data transmissions in WSN



3.2.2 Protection schedule

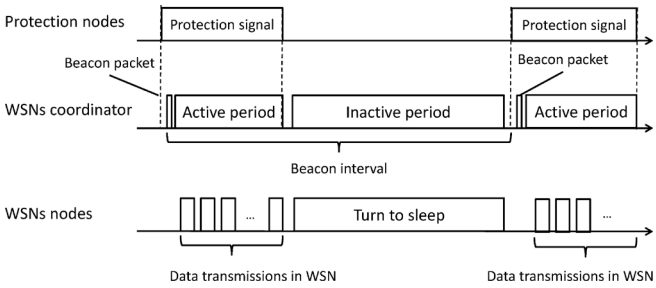
To coordinate the communications in WSNs, the coordinators broadcast periodically the working schedules by beacon packets. An example is shown in Figure 3. The working schedule is divided into two periods: active period and inactive period. In active period, by receiving a beacon, WSN nodes will adjust their duty cycles according to the working schedule so that the network can work synchronously. WSN nodes communicate with each other by following slotted-CSMA. In inactive period, WSN nodes will turn into sleeping mode.

Figure 3 Working schedule of WSN



Our protocol will exploit the beacon packets in the WSNs to synchronise the protection nodes and the WSNs nodes. Before the beginning of WSN transmissions, all protection nodes keep on listening until they receive the first beacon packet from the nearby WSN nodes, and they will emit protection signals in active period and keep silence in inactive period. It is crucial to protect the transmission of beacon packets in a multi-hop WSN, because the coordinator will use beacon packets to control network topology, synchronise with other nodes, and perform neighbour discovery, etc. To ensure that the protection nodes and WSNs nodes can receive beacon packets, the protection nodes will emit protection signal a little earlier than the beginning of beacon packets transmission to obtain more efficient protection in hybrid network communications. An example is shown in Figure 4.

Figure 4 The time sequence for protection nodes, WSN coordinator, and WSN nodes



By overhearing the regular beacon packets, the protection nodes can be synchronised easily with the WSNs nodes by the working schedule and provide transmission protection. Protection nodes will emit protection signal in every WSN active period. At the end of each WSN active period, protection nodes will cease the emission of protection signal so that the WLAN can access the channel to perform or recover immediately data transmission by its aggressive time resolution. Besides, WSNs are targeted at low data rate applications whose typical low duty cycles

vary from 1% to 10% (IEEE 802.15 Working Group, 2010). So that, with a carefully determining duty cycle, the performance of WLAN will not be affected virtually by WTPP.

4 Implementation

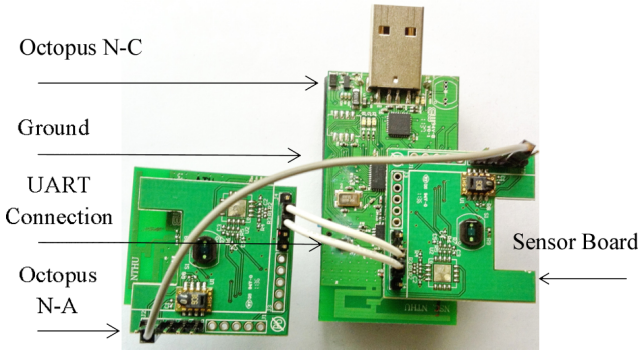
We verify the effectiveness of our protocol by two testbed experiments based on both Octopus N series (http://hscc.cs.nthu.edu.tw/) and GNURadio/USRP N200 software radio platform (http://www.gnuradio.org). To evaluate the feasibility of WTPP, we implement the protection node prototypes based on the Octopus N series and set up a testbed to evaluate the performance of WTPP. In further experiments, we use GNURadio/USRP N200 software radio platform to emit protection signal, instead of protection nodes, to provide more powerful protection and evaluate the performance of WTPP again.

4.1 Protection node

We implement the protection node prototype with an Octopus N sensor board, an Octopus N-C node and an Octopus N-A node, which are designed and developed by High Speed Communication and Computing (HSCC) laboratory, National Tsing Hua University in Taiwan.

The Octopus N series are a series of low-power wireless communication platforms, which are compatible with the IEEE 802.15.4 standard. They can support the ZigBee protocol and are suitable to WSNs applications. The Octopus N-A and Octopus N-C are equipped with Texas Instrument CC2530 radio chip, PCB antenna and UART interface. Furthermore, the Octopus N-C has an external signal amplifier, 2 MB external flash memory space, a Micro SD socket and a USB interface. The Octopus N sensor board can be equipped with multiple sensors and a pin expansion connector, by which the microcontrollers on Octopus N-A and Octopus N-C can communicate with each other directly via the UART interface. Figure 5 shows the picture of the protection node prototype.

Figure 5 The protection node prototype (see online version for colours)



We choose Octopus N-C to emit the protection signal because of its greater transmission power. In the aim of reducing the response time on Octopus N-C, we use C language program to control the microcontroller directly instead of running an operating system on it. Ideally, by controlling the radio chip on Octopus N-C directly, we can send packets back to back and occupy the channel continuously. On the other hand, we run Texas Instrument z-stack on Octopus N-A. Z-stack is a ZigBee-compatible protocol stack. The microcontroller on Octopus N-A works as a master, which can inform the Octopus N-C perform the desired operations.

In experiments, the Octopus N-A will keep listening until it receives the first beacon packet. After it receives a beacon packet, it will interpret and transmit the WSN working schedule in beacon to Octopus N-C via the UART interface. The Octopus N-C will send the protection signal according to the schedule also. The protection signal will be a little earlier than the beginning of next beacon interval to protect the coming beacon packet.

4.2 Testbed

We set up a testbed for WTPP, which consists of a WSN and a WLAN. The WSN nodes and the protection node prototype Octopus N-C work on channels 23 and 22 under IEEE 802.15.4, respectively, and the WLAN devices work on channel 11 under IEEE 802.11n. The channel of WLAN overlaps with the channels of WSN and the protection node. Moreover, the transmission power, CCA operation threshold and backoff mechanism of both WSN and WLAN are fixed. We run ZigBee protocol on Octopus N-A nodes to simulate an environment monitor, and use a D-Link DIR-635 wireless device as a WLAN AP. To generate WLAN traffic, we connect a laptop computer to the AP. In addition, we put a sniffer in the testbed, which can record the activities on the target frequency band and give the trace information of our testbed experiments. We also install a software network traffic monitor on the laptop computer so that we can have a clear observation of the impact on the WLAN. The execution time of each experiment is 5 min.

4.3 Experiments process

At the beginning, the laptop computer is connected to the WLAN AP and transmit a file via FTP at the speed of 16 Mbps. Simultaneously, the WSN coordinator broadcasts beacon packets periodically. Upon receiving the beacon packets, WSN nodes will reply 80-byte data packets to the WSN coordinator in active periods. During each experiment, the WSN coordinator counts how many packets it receives and the WSNs nodes count how many packets they have sent. At the end of the experiment, we can calculate the packet loss rate by the number of packets received and sent.

4.4 Comparison

We first run legacy ZigBee protocol to get a baseline for later comparison. After that, we put two protection nodes

into the WSN and run experiments all over again. In the end, we compare the results and evaluate the performance of WTPP. Moreover, our software traffic monitor will reveal the impact of protection signals on the WLAN.

5 Performance evaluation

The performances of WTPP are evaluated by not only the protection nodes based on Octopus N series but also the GNURadio/USRP N200 software radio platform in a real-world testbed.

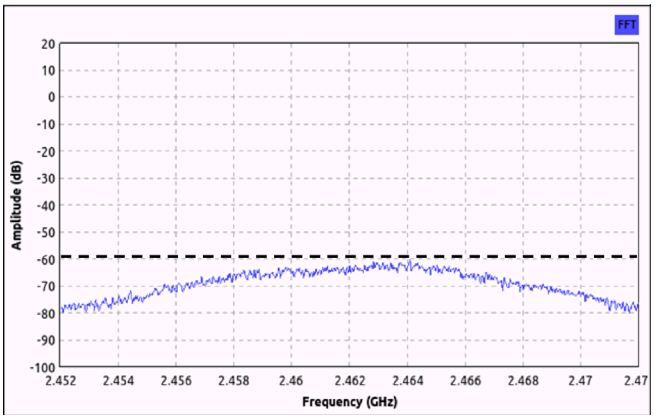
5.1 Protected by protection node

In the part of hybrid network communication performance evaluation based on protection nodes, we will focus on the performance of the transmission protection for WSNs, and the impact on WLANs devices from protection signals.

5.2 Transmission protection for WSNs

First, we will examine the effectiveness of protection signal sent by the protection nodes. Figure 6 presents the average RSSI on the sniffer when the target channel is clean, while there are no activities in the WLAN or WSN. It is shown that it is below −60 dB, which is regarded as a baseline.

Figure 6 The average RSSI on the sniffer during a clean channel period (see online version for colours)



In Figure 7, we use notebook laptop computer to transfer a big enough size file at the speed of 16 Mbps. At the same time, the WSN still works. It is shown that after the traffic of WLAN is activated, the average RSSI rises above the baseline and can be up to −30 dB, which level of power can easily make WSNs nodes backoff. With an intense traffic of WLANs (>8 Mbps), the communication of WSN nodes nearby will suffer from high packet loss rate (>35%).

In Figure 8, we start the emission of protection signal, and the traffics in the WLAN are suppressed below the baseline. As a result, the WSNs nodes can transmit packets without interference. It is shown that only two peaks sent by Octopus N-C nodes and WSN nodes are over the baseline.

In the following evaluation, the duty cycle of WSN is set to 10%. The WSN coordinator broadcasts a beacon packet per two seconds to synchronise the working schedule of WSN nodes and the protection nodes. The speed of WLAN traffic is also set to 16 Mbps.

Figure 7 The average RSSI when there are WLAN activities in the frequency band (see online version for colours)

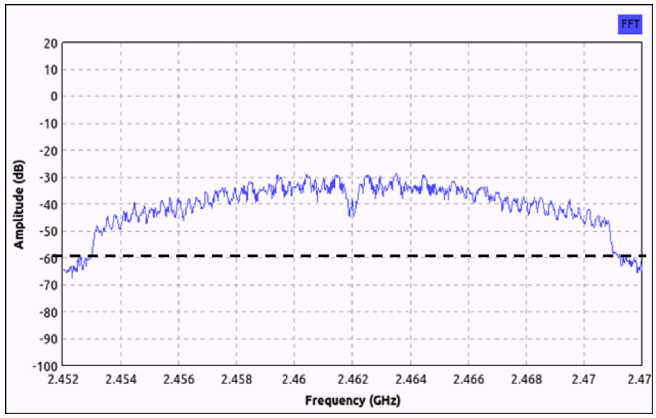
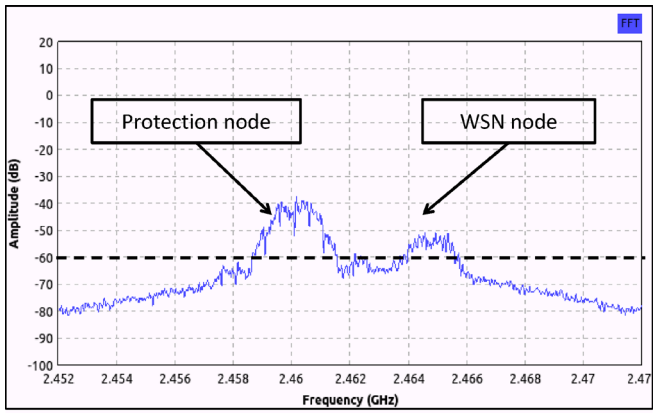


Figure 8 The average RSSI when there are WLAN, WSN and protection nodes working simultaneously (see online version for colours)

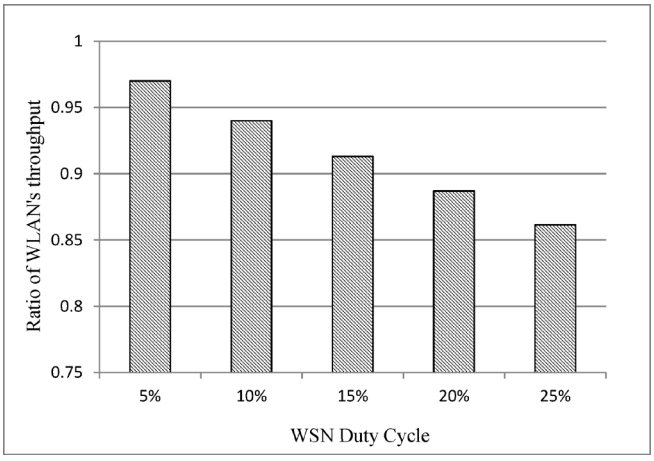


The average experimental results show that the legacy ZigBee protocol suffer from high packet loss rate (>53%), but WTPP can improve the packet delivery ratio of WSN from 47% to 86%. Compared with legacy ZigBee, in another word, WTPP outperforms ZigBee by 1.8 times on the packet delivery ratio of WSN. In an ideal state, the transmission in WSN will keep being protected when the protection signal exists. However, in fact, the transmission power of Octopus N-C is approximately 10 dB lower than WLAN devices. Because of its insufficient transmission power, protection node cannot suppress the WLAN traffic immediately. To solve this problem, we make the protection nodes emit protection signal 200 ms earlier than the upcoming WSN active period to occupy the channel ahead of schedule. Actually, this compromise caused by the insufficient transmission power can be solved by providing higher transmission power on protection nodes.

5.3 Impact on communication of WLANs

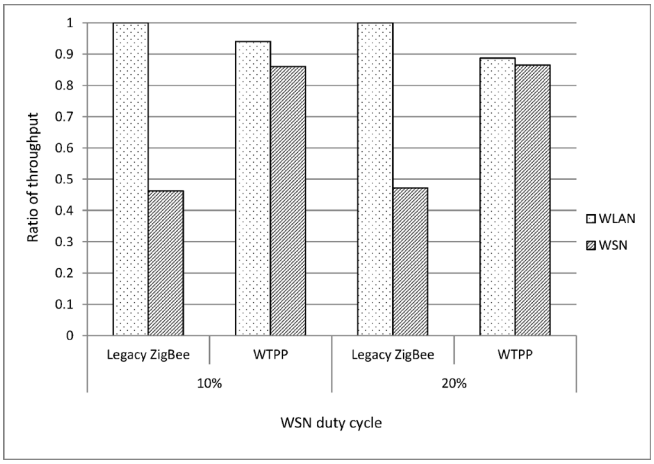
In the second experiment, we try to find out the impact of protection signal on WLAN. By our protection mechanism, the duty cycle of WSN determines the amount of time that WLAN devices are suppressed, so we keep the two seconds of beacon interval and change the duty cycle of WSN. The average result is shown in Figure 9. The ratio of WLAN's throughput is 1 when the protection nodes do not work. When the protection nodes begin to send protection signals and the duty cycle of WSN is 5%, the ratio of throughput degradation of WLAN is only 3%. As the duty cycle of WSNs increases, the impact of protection signal on WLANs will also increase. Because the transmission power of Octopus N-C cannot make the traffic of WLAN backoff completely, the traffic of WLAN has small chances to access to its work channel under the protection signal. Moreover, owing to the more aggressive time resolution of WLANs, WLANs can access its work channel immediately after the protection nodes stop sending the protection signal.

Figure 9 The ratio of WLAN's throughput against different duty cycles in WSN



In Figure 10, we compare the ratio of WLAN's throughput and WSN's throughput when the WSN runs legacy ZigBee protocol and WTPP with different duty cycles, respectively. When the WSN runs legacy ZigBee protocol, the throughput ratio of WLAN is virtually unaffected (>99%) and the throughput ratio degradation of WSN will not be affected by the change of its duty cycle; with the same traffic in WLAN, the packet delivery ratios of WSN under different duty cycle are same (≈47%). Under the protection of WTPP, the packet delivery ratios of WSN with different duty cycles are almost also same (≈86%). The throughput degradations of WLAN are only 6 and 11% when the duty cycles of WSN are 10 and 20%, respectively, so that we can conclude that WTPP can improve the throughput of WSN with a few degradations on the throughput of WLAN. In another word, with a small recession of the WLAN's throughput, the throughput of WSN can be improved dramatically. Thus, the WSNs and WLANs are able to coexist in a better trade-off situation by WTPP.

Figure 10 The ratio of throughputs of WLAN and WSN when running legacy ZigBee and WTPP, respectively



5.4 Protected by USRP

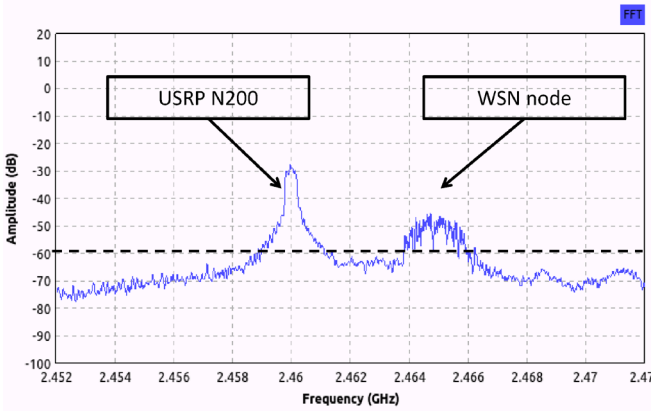
In the previous experiments, we use Octopus N-C to protect the transmission of WSN and find out the power of its protection signal is not enough to suppress WLAN perfectly. To provide sufficient protection power, we use GNURadio/USRP N200 software radio platform to emit the protection signal instead of Octopus N-C. We design to program on USRP N200 to send protection signal at a desired frequency centre in an adjustable frequency bandwidth. By controlling the length of protection packets, we can easily adjust the protection period. However, during the implementation, we find that USRP N200 could not emit protection signal at a desired frequency centre perfectly. If we follow IEEE 802.15.4 standard and set the bandwidth of protection signal to 4 MHz, it is commonly observed that the protection signal will suppress the transmission not only in WLAN but also in WSNs that are on the adjacent channel. A straightforward way to solve this problem is to shift the frequency centre of protection signal to the left-side channel of WSN transmission or to use narrower frequency band. For example in Figure 2, since the frequency centre is 2.445 GHz, we can shift WSN transmission to channel 21. Moreover, after a series of experiments, we decide to send the protection signal on 2.46 GHz and set the bandwidth to 2 MHz.

In Figure 11, we can clearly see that when the USRP N200 sends out the protection signal, the data transmissions in WLAN are suppressed successfully. At the same time, the protection signal will not interfere with the data transmissions in WSN. Because of the greater transmission power, USRP N200 is able to suppress the transmission in WLAN more effectively and improve the packet delivery rate of WSN from 47% to 97%. Compared with legacy ZigBee, the improvement is 2 times better. Although USRP N200 can suppress WLAN traffic effectively, the transmissions in WSN have still small chance (2.6%) to

collide with the WLAN control packets, which are sent without carrier sensing.

By the above-mentioned testbed experiments, it reveals that the idea of using protection signal to protect the data transmissions in WSNs under WLANs' interference is highly feasible. Moreover, we find out that the transmission power of the protection node is the most important role on protecting the data transmissions in WSNs.

Figure 11 The average RSSI when WLAN, WSN, and USRP N200 are working in the same time (see online version for colours)



6 Conclusion

Traditionally, packet acknowledgement and auto packet retransmission mechanisms are used to solve the confliction problem in coexistence environment of WSNs and WLANs. However, the communications performances of WSNs will still be severely degraded when coexisting with WLANs in hybrid networks because of WLANs devices' greater transmission power and more aggressive time resolution for channel access. When the interference from WLANs increases, the packet loss rate of WSNs will increase drastically and it will waste more energy on packet retransmissions. In this paper, we propose a WTTP to harmonise the coexistence between WSNs and WLANs. Our protocol uses protection nodes to emit protection signal to protect the data transmission of WSNs simultaneously. The protection signal is able to enhance the visibility of the WSNs data transmissions in WLANs and prevents WLANs to interrupt the ongoing transmissions in WSNs. We implement protection nodes prototype based on Octopus N series wireless devices and USRP N200. Our protocol can achieve 1.8 times better on packet delivery ratio of WSNs than legacy ZigBee protocol under high traffic rate in WLANs. Moreover, the throughput of WLANs has negligible decrease (<6%) when our protection protocol runs in low duty cycle (<10%) in WSNs applications. In brief, WTPP can help communication of WSNs to accomplish high data transmission rate in the interference of WLANs, with less throughput degradation on WLANs.

References

Crossbow Technology Inc. (2004) *Avoiding RF Interference between WiFi and ZigBee*, Technical Report.

Gummadi, R., Balakrishnan, H. and Seshan, S. (2009) 'Metronome: coordinating spectrum sharing in heterogeneous wireless networks', *Proceeding of the First International Conference on Communication Systems and Networks*, January, Bangalore, India, pp.157–166.

Guo, W., Healy, W.M. and Zhou, M. (2011) 'Interference impacts on ZigBee-based wireless mesh networks for building automation and control', *Proceeding of the Conference on Systems, Man, and Cybernetics*, October, Anchorage, Alaska, USA, pp.3452–3457.

Hauer, J-H., Handziski, V. and Wolisz, A. (2009) 'Experimental study of the impact of WLAN interference on IEEE 802.15.4 body area networks', *Proceeding of the 6th European Conference on Wireless Sensor Networks*, February, Cork, Ireland, pp.17–32.

Huang, J., Xing, G. and Zhou, G. (2010) 'Beyond co-existence: exploiting WiFi white space for ZigBee performance assurance', *Proceeding of the 18th IEEE International Conference on Network Protocols*, October, Kyoto, Japan, pp.305–314.

IEEE 802.11 Working Group (2009) *IEEE Standard for Information Technology – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancement for Higher Throughput*, IEEE Std.802.11n, October.

IEEE 802.15 Working Group (2003) *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Std 802.15.4, October.

IEEE 802.15 Working Group (2010) *Coexistence Analysis of IEEE Std 802.15.4 With Other IEEE Standards and Proposed Standards*, IEEE 802, September.

Liang, C-J.M., Priyantha, N.B., Liu, J. and Terizs, A. (2010) 'Surviving WLAN interference in low power ZigBee networks', *Proceeding of the 8th ACM Conference on Embedded Networked Sensor Systems*, November, Zurich, Switzerland, pp.309–322.

Liu, S., Xing, G., Zhang, H., Wang, J., Huang, J., Sha, M. and Huang, L. (2010) 'Passive interference measurement in wire-less sensor networks', *Proceeding of the 18th IEEE International Conference on Network Protocols*, October, Kyoto, Japan, pp.52–61.

Musåloiu-E., R. and Terzis, A. (2008) 'Minimising the effect of WIFI interference in 802.15.4 wireless sensor net-works', *International Journal of Sensor Networks*, January, Bologna, Italy, pp.43–54.

Oliveira, L.M.L., Rodrigues, J.J.P.C., Mação, B.M., Nicolau, P.A. and Zhou, L. (2012) 'A WSN solution for light aircraft pilot health monitoring', *Proceeding in Wireless Communications and Networking Conference*, April, Shanghai, China, pp.119–124.

Won, C., Youn, J-H., Ali, H., Sharif, H. and Deogun, J. (2005) 'Adaptive radio channel allocation for supporting coexistence of 802.15.4 and 802.11b', *Proceeding of the 62nd IEEE Vehicular Technology Conference*, September, Dallas, USA, pp.2522–2526.

Zhang, X. and Shin, K.G. (2011) 'Enabling coexistence of heterogeneous wireless systems: case for ZigBee and WiFi', *Proceeding of the 12th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, May, Paris, France, Article No. 6.

Websites

Low-power Wireless Communication Platform: Octopus N, Available: http://hscc.cs.nthu.edu.tw/

The GNU Software Radio, Available: http://www.gnuradio.org