

A Lightweight and Robust Interference Mitigation Scheme for Wireless Body Sensor Networks in Realistic Environments

Shipeng Liang^{1,2}, Yu Ge², Shengming Jiang³, Hwee Pink Tan²

¹South China University of Technology, Email: [sp.liang887]@gmail.com

²Institute for Infocomm Research, Singapore, Email: [geyu, tanhp]@i2r.a-star.edu.sg

³Shanghai Maritime University, Email: smjiang@shmtu.edu.cn

Abstract—In dense deployments of Wireless Body Sensor Networks (WBSNs), inter-user interference significantly degrades network performance when multiple WBSN users stay in a small area such as hospitals. Due to the high dynamics of the environments, it is usually hard to schedule the transmissions of multiple WBSNs without a central controller. In this paper, we propose a robust and lightweight interference mitigation scheme for realistic WBSN systems through adaptive channel hopping. A WBSN testbed is set up to investigate the impact of inter-user interference on various performance metrics when different severity levels of interference are present. Based on the measurement results, we propose a distributed interference detection and mitigation scheme without any central controller. A WBSN prototype system has been set up and shown that our proposed scheme can effectively detect and mitigate the multi-user interference, with tripling the network throughput in severely interfered environments.

Keywords—Wireless Body Sensor Network; IEEE 802.15.4; Interference Detection; Interference Mitigation; Transmission Efficiency

I. INTRODUCTION

Wireless Body Sensor Networks (WBSNs) have recently attracted much attention due to their high potential to be used in many human-centric applications in healthcare, fitness, sports training, entertainment, and military operations. In realistic deployment cases, multiple WBSN users may stay in a specific small area such as a hospital ward and sports field. Due to the broadcast nature of wireless transmissions, inter-user interference, caused by concurrent transmissions from multiple WBSN users, usually leads to the degradation of network performance such as throughput, delay, and energy efficiency. As a consequence, the service quality is compromised and hard to support strict requirements of human-centric applications.

As the performance degradation is possibly caused by inter-user interference and/or deteriorated channels when body posture changes, it is important to detect the actual causes and find suitable solutions accordingly. For example, if the performance is degraded due to deteriorated channels, an effective method would be increasing transmission powers or transmitting via a relay node. However, if inter-user interference causes performance degradation, the above

methods are not able to effectively improve the performance, and hence an interference mitigation scheme is necessary in this situation.

In this paper, we focus on designing an effective scheme to detect and mitigate the inter-user interference. Our work is significantly different from earlier related research in the literature, as our approaches for detecting and mitigating interference are distributed, without the need of a central infrastructure or message exchanges among WBSN users. In addition, our work is based on a realistic WBSN system instead of simulation platforms. Our main contributions in this paper are as follows. Firstly, we present the empirical evidence through extensive experiments, to show the impact of inter-user interference on various network performance metrics. Secondly, from the above results, we propose a method to effectively detect the severity level of inter-user interference. Thirdly, we propose a lightweight and robust scheme to mitigate inter-user interference through distributed channel hopping, according to the severity of the interference. Lastly, we implement the proposed schemes on a CrossBow MicaZ-based WBSN system and evaluate the performance through extensive experiments¹.

The rest of the paper is organized as follows. Section II describes the related research. Section III presents the performance indicators for inter-user interference and the design of channel hopping schemes. Section IV presents the experiment results to evaluate the performance of the proposed interference mitigation scheme. Finally, Section V concludes the paper.

II. RELATED WORK

Much research work has been published to address interference issues for wireless networks. Liu et. al. presented a passive interference measurement approach [1] by measuring packet-level interference from neighboring nodes. In [2], Son et. al. proposed a transmission power control mechanism incorporating blacklisting channel to minimize interference.

¹ We implemented our schemes on the TKN MAC developed by Technical University Berlin in this research.

Yoon et. al. proposed an adaptive channel hopping scheme [3] to dynamically switch channels based on the decrease of link quality indicator (LQI). However, according to our experimental results, LQI is usually sensitive to link quality changes, e.g. due to posture changes, but not sensitive to interference. Therefore, LQI may not be a good interference indicator in realistic systems. Peng and Roussos proposed an adaptive channel hopping scheme [4], which uses both packet delivery ratio (PDR) and expected transmissions (ETX) as indicators of inter-user interference. However, from our experimental results, when interference is present, network throughput may significantly decrease, but PDR still possibly maintain satisfactory levels when operating in well-designed contention based MAC [5]. The most relevant work was reported in [6]. In this paper, the authors conducted a preliminary investigation of the impact of inter-user interference with a simple configuration, and then proposed to deploy a fixed infrastructure to assign the channels to users.

To address the inter-user interference in WBSN, we conducted a case study in hospital deployment scenarios [7]. Based on the results, we proposed a lightweight method to shift the beacon of each WBSN to avoid collisions in low duty-cycle operations [8], as well as a simple method to conduct channel hopping in severe interference situations [5]. To enhance the robustness of interference mitigation schemes and reduce the overhead in communications and computation, in this paper, we propose a distributed and robust interference mitigation scheme, which is able to detect the interference on-the-fly and make fast decision on channel hopping.

III. COMMUNICATION MODE AND PERFORMANCE INDICATORS

A. Communication Mode

A WBSN usually consists of a coordinator, which controls network operation and data collection, and several sensor nodes, which transmit the collected vital sign data to the coordinator. In our work, the beacon-enabled superframe mode in IEEE 802.15.4 standard is adopted. In the beacon-enabled mode, the coordinator periodically broadcasts beacons. Upon reception of a beacon, the nodes in this network are allowed to send packets in the active period of this superframe. As shown in Figure 1, a superframe contains contention access period (CAP) and contention free period (CFP) in its active period. Sensor nodes are in sleep mode in the inactive period. In CFP, a node sends packets in the slots allocated by the coordinator without contention.

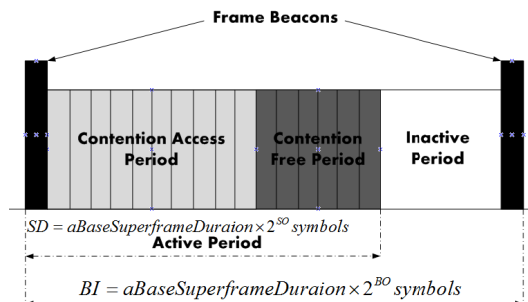


Figure 1 Superframe structure in IEEE802.15.4.

During CAP, a node must scan the channel to detect idle slots for its transmissions. If signals are detected, the node has to back off for a random period and conduct carrier sensing again until it detects the channel being available for transmission. Retransmissions will be carried out in the case of failed transmissions. In this research, we focus on CAP in beacon-enabled mode as the majority of the packets, unless carrying urgent information, are transmitted in CAP.

B. Impact of Interference on Performance

As performance degradation in WBSN is possibly caused by deteriorated channels and/or inter-user interference, accurately detecting the severity of inter-user interference is critical in order to improve network performance using suitable schemes. To this end, we investigate the following performance metrics with extensive experiments in WBSN testbed with the presence of different severity levels of interference.

Throughput is the total number of packets successfully received at the coordinator during a certain period. It is a primary indicator for interference detection, as the throughput drops rapidly when interference is present.

Beacon delivery ratio (BDR) is the percentage of beacons successfully received by a sensor device. In a beacon-enabled MAC, beacons are usually transmitted at the scheduled time with a fixed interval (superframe length) without collision avoidance mechanism. Therefore, beacon collisions happen frequently in an interfered channel, and a node is not able to transmit data in a superframe without receiving a beacon.

Number of backoffs per successful packet measures the number of failed trails by a node to access the channel before it actually transmits a packet. In CSMA/CA, a device has to conduct carrier sense to ensure that the channel is idle before sending a data packet. When multiple users concurrently transmit in the same channel, a node usually has to back off a few times before transmission. As such, the number of backoffs indicates the utilization of the channel.

Number of transmissions per successful packet measures the total number of transmissions required to deliver a packet successfully. A failed transmission will trigger retransmissions until the pre-configured maximum retransmission limit is reached. The number of transmissions per packet may increase significantly when multiple users transmit in the same channel.

Received signal strength indicator (RSSI) measures the signal strength of a packet when it reaches the receiver, and thus it is used to represent the link quality. In WBSNs, human body usually has great shadowing effects on radio propagation, which possibly leads to significant variations of RSSIs and performance degradation for on-body links. However, our experimental results show that interference does not have obvious impact on RSSI, and hence the RSSI can be used to differentiate the scenarios of interference and bad link quality.

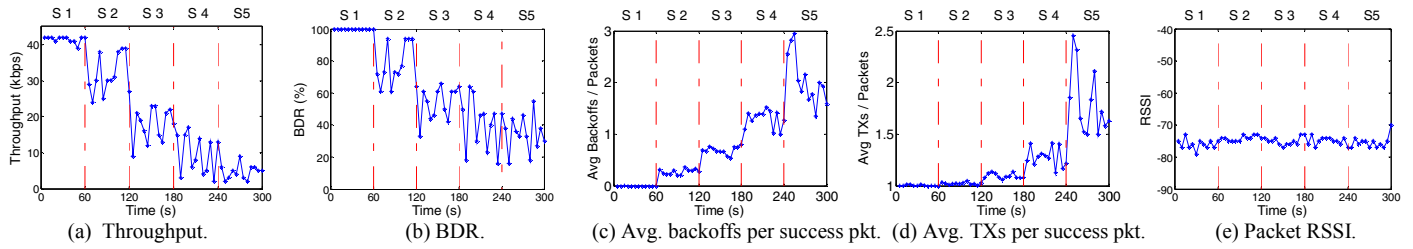


Figure 2 Performance metrics affected by interference in on-table experiments. Scenario 1 to Scenario 5 (S1 to S5) represent no jammer and 1-4 jammers scenarios.

In order to select appropriate metrics for interference detection, we investigate the impact of interference on the above metrics with different experimental settings.

i). Impact of interference under perfect channel conditions (On-table experiment)

We first conduct on-table experiments in order to observe the impact of interference under perfect channel condition. A sender and a receiver are deployed 60 cm apart on a table. Four jamming nodes are deployed in the middle of the sender and receiver, and all nodes operate in the same channel. The sender transmits packets with 110-byte payload every 20 ms during the CAP in IEEE 802.15.4 beacon-enabled mode, where slotted CSMA/CA is applied for channel access. The jammers simply send 110-byte packets every 20 ms without channel sensing. The experiments are conducted in a MicaZ based WBSN testbed, running TinyOS 2.x Operating System. The performance metrics are recorded every 5 s at the nodes.

We first turn on the sender and receiver, and then turn on a jammer after every one minute. The results are shown in Figure 2. When more and more jammers are active, the network throughput drops consecutively in Scenario 2 to 5 (S2 to S5), where one to four jammers are active, respectively (see Figure 2(a)). As shown in Figure 2(b), BDR declines as more beacons collide with jamming signals. It can be observed that BDR is very sensitive to interference from external transmitters, as there is no carrier sense before beacon transmissions.

As shown in Figures 2 (c) and (d), for each successful packet, both the number of backoffs and the number of transmissions significantly increase from S1 to S5, implying that they are significantly affected by interference. A node probably has to sense the channel a few times before its actual transmission due to the heavy utilization in the channel in S2 to S5. Similarly, the number of transmissions for a successful packet increases when more jamming signals are present, which, in turn, explains the consecutive drops in throughput in the scenario 2 to 5. However, the RSSIs of data packets are not sensitive to interference, as shown in Figure 2 (e), but very sensitive to body movements with up to 30 dB variation [9].

In summary, all the above performance metrics, except packet RSSI, are sensitive to inter-user interference, and can be used as interference detector in a combinational manner.

ii). Impact of interference under dynamic channel conditions (On-Body Experiment)

To investigate the impact of inter-user interference on the performance metrics in realistic WBSNs, we conduct experiments with the following two scenarios²:

Scenario 1: a WBSN user wears a coordinator on the left waist and two sensor nodes on both arms as in Figure 3 (a). The user walks randomly in a room with 10m x 10m dimension. The results in Scenario 1 provide a benchmark performance as a reference to the analysis of performance in Scenario 2.

Scenario 2: five WBSN users and three human jammers, each wearing the same set of WBSN devices as Scenario 1, walk in the same room randomly. Nine static jammers are uniformly deployed on the table in the room to emulate the dense deployment scenario. All devices operate in the same channel. This scenario is shown in Figure 3 (b). The rest of the experimental settings are the same as the on-table experiments. In Scenario 2, we first turn on all jammers, and then turn on the devices on WBSN users.



(a) Locations of on-body nodes. (b) Multiple-user experiment.

Figure 3 Experiments for on-body performance study.

The performance results of the observed user are shown in Figures 4 for Scenario 1. As depicted in Figure 4 (a), the throughput of a device can reach near 40 Kbps at left arm position (with good link quality); and near 30 Kbps at right arm position (with boundary-level link quality). The difference in performance of the two nodes is caused by different link quality. Nevertheless, the BDR of both devices can reach 90% level in Scenario 1, when there is no external interference.

Comparably, Figure 5 shows the performance results of the same WBSN user in Scenario 2. Compared to the one-user scenario, when there are five users and a couple of jammers in the same room, a single user can only achieve up to 7 Kbps throughput, around 1/6 of the throughput in Scenario 1.

² Due to space limit, we only present the scenario when severe interference is present and omit the data with different levels of interference scenarios.

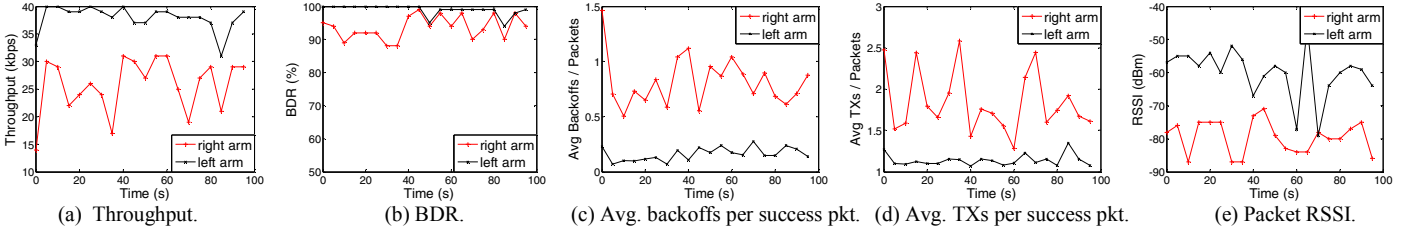


Figure 4 Performance results in one-WBSN scenario (Scenario 1).

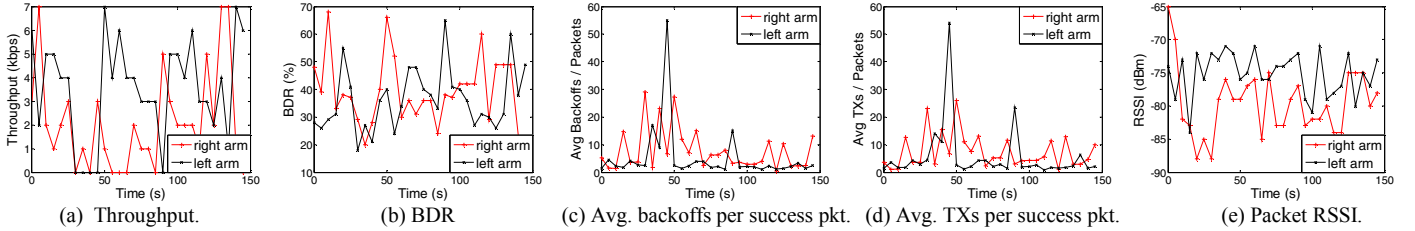


Figure 5 Performance results in multiple-WBSN scenario (Scenario 2).

In our experimental study, if there is only one active WBSN, the BDR of all nodes can achieve at least 90%, and the BDR does not decrease regardless of the number nodes in the WBSN³. However, in multi-user scenario, the BDR can drop to 20% (see Figure 5 (b)), even when the link quality is good (RSSI > -85 dBm), which shows the significant impact of inter-user interference on BDR. Therefore, BDR is a good indicator to detect inter-user interference.

The average number of backoffs per successful packet is calculated from dividing the total number of backoffs in a 5 s window by the total number of packets successfully received during the same window. The average number of transmissions per successful packet is also calculated in a 5 s window. From Figures 4 (c) and (d), in Scenario 1, the above two metrics are more stable and much lower at the node at left arm, as compared to the node at right arm, which is caused by the link quality difference. In the multi-user scenario, however, the two metrics are much higher (see Figures 5 (c) and (d)) than the one-user scenario. Obviously, the greater backoffs and retransmissions are caused by severe interference, as both links show sufficiently good quality for successful transmissions (see Figures 5 (e)). We also observe that link quality can be easily affected by moving body, which leads to RSSI variations (see Figures 4 (e) and 5 (e)). However, the RSSI is not sensitive to interference (see Figure 2(e)). Hence, RSSI can be used as an auxiliary parameter for interference detection.

In summary, from our experimental study, the combinational analysis of throughput, BDR, the average number of backoffs and transmissions per successful packet, as well as RSSI, can provide good indications for inter-user interference.

IV. INTERFERENCE MITIGATION SCHEME

Based on the experimental study of interference indicators, we propose a lightweight and robust interference detection and mitigation scheme through channel hopping. The functional

modules at the coordinator and the sensor device are shown in Figure 6. The procedure of the proposed scheme is described as follows:

Step 1 (Interference Detection): During data transmissions, each sensor node monitors on-the-fly the performance metrics in terms of BDR, average number of backoffs and transmissions, and RSSI. From the collected performance data, it evaluates the severity of interference using our proposed interference detection scheme. Once the severity of interference is identified to be beyond the pre-defined threshold, the sensor node sends a channel hopping request to the coordinator, indicating the needs for hopping (see Section IV.A for details).

Step 2 (Interference Computing): The coordinator records the number of hopping requests from different nodes and computes the severity level of interference in its network. Once the coordinator identifies the needs of channel hopping from the fusion of the collected requests, it sends a scanning request to a selected sensor node, to request the node to seek for a good channel for hopping (see Section IV.B for details).

Step 3 (Channel Inspection): The selected node, called *watcher*, scans the channels and finds a good target channel. It then reports the information to the coordinator.

Step 4 (Channel Hopping): Once the coordinator gets the report from the watcher, the coordinator informs its network the target channel, and then switches to the new channel.

A. Interference Detection

To measure the interference, a sensor node has to calculate multiple metrics as indicators. First, BDR is calculated based on a fixed window to ensure sufficient accuracy. In our study, the sampling window is configured to be 5 s (20 superframes). To smooth out the instantaneous variations, we use the exponential averaging method to estimate BDR at time t , as

$$\hat{B}_t = B_t \times \alpha + \hat{B}_{t-1} \times (1 - \alpha) \quad (1)$$

Where \hat{B}_t and \hat{B}_{t-1} are respectively the estimated BDR at time t and $t-1$, B_t is the sampled BDR in the current window, and the smoothing factor α is set to 0.8 in our experiments.

³ We tested the cases with 1-8 sensor nodes in a WBSN. Such results are not presented due to space limit.

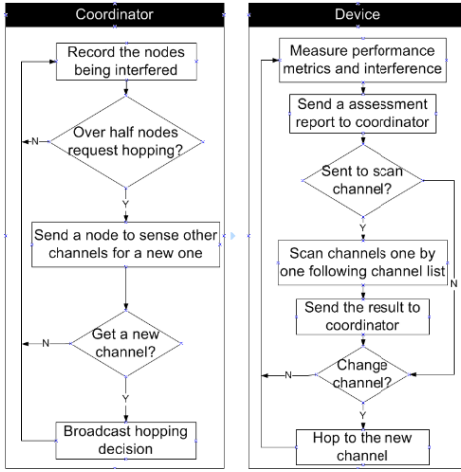


Figure 6 Functional modules of interference mitigation scheme.

From our quantitative studies at various severity levels of interference, the suitable BDR threshold is 70% for design of channel hopping. If BDR drops below this threshold, channel hopping is necessary to maintain the acceptable performance.

From our measurement results, BDR is vulnerable to external interference and shows great variations even with the presence of light interference. To detect the severity of interference in a more robust way with multiple performance metrics, we define the *Transmission Efficiency*, TE , as:

$$TE = \frac{P}{P + B + R} \quad (2)$$

Where P is the number of packets successfully received; B and R are respectively the number of backoffs and retransmissions. All the metrics are measured over a fixed window. TE is designed to indicate the severity of interference, where the smaller TE indicates the more severe level of the external interference, and hence the lower efficiency in transmissions. The threshold of TE is configured according to the strictness of the application requirements.

In addition, the RSSI of a packet can be obtained at the moment of packet reception to provide link quality information. From our experimental results, RSSI is significantly affected by user movement and multi-path from environments, but not obviously affected by interference, and hence the RSSI can be used to as one of the indicators to differentiate the scenarios of interference and bad channels.

In summary, with the combinational analysis of BDR, TE , and RSSI, the severity of interference can be robustly detected. When the throughput drops significantly, and both BDR and TE are lower than their thresholds but the RSSIs show good link quality, it implies the presence of severe interference and channel hopping is necessary. Once a sensor node detects such a situation, it immediately sends a channel hopping request, embedded in the MAC header, to its coordinator.

B. Channel Hopping Decision and Operation

The coordinator records the channel hopping requests from its sensor nodes within a valid duration. As long as more than half of the nodes in the WBSN have requested channel hopping, the coordinator determines the necessity to switch channel. The coordinator then selects one node as the watcher to conduct channel sensing to find the target channel to switch to. In our design, the watcher is the sensor node with high RSSI and low traffic load, so that it can smoothly communicate with the coordinator without compromising its own transmission.

Upon the request, the watcher scans the channels sequentially, according to the channel list hashed by the unique network ID. Energy Detection method is used in channel scanning. According to the standard as well as the hardware profile, the energy detection threshold is -77 dBm to differentiate noise and transmission signals. The watcher scans a channel for 32 times during two superframes, and calculates the utilization of the channel based on the threshold. Once a channel is detected in low utilization, the watcher reports the channel ID to the coordinator as the target channel. The coordinator then sends a realignment frame to its sensor nodes, indicating the new channel to switch to. Receiving the realignment frame, the node switches to the target channel. In the case of a node losing the realignment frame and subsequently losing the synchronization with the coordinator, the node will scan the beacons in the list of channels to re-connect to the coordinator.

V. PERFORMANCE RESULTS

In this section, we conduct extensive experiments to evaluate the effectiveness of our proposed interference mitigation scheme. The configurations of the experiment are as follows. Nine static jammers operate in three channels (Channels 12, 18, and 24), three for each channel, to emulate static users in realistic environments. Three mobile WBSNs are deployed as mobile jammers, operating in Channel 23, while moving randomly in the meeting room. Five WBSN wearers move randomly in the meeting room, each WBSN starts its transmissions at a different schedule as shown in Table I. The five observed WBSNs enable the interference mitigation scheme, and their performance metrics are recorded during the experiments. The interference mitigation scheme is disabled in both static and mobile jammers, so that the jammers stick to their pre-configured channels during the experiment. Both WBSN nodes and jammers transmit 110-byte packets at 20 ms interval and the whole experiment lasts for 8 minutes.

When the experiment starts, we first turn on all jammers; the mobile jammers start to move randomly in the meeting room. Then, the five observed WBSNs are turned on at their pre-specified time, and transmit in their pre-defined initial channels. They move randomly in the meeting room and their channels are recorded during the experiment, as shown in Table I.

In the experiment, WBSN1 is activated firstly and transmits in Channel 23. After a while, WBSN1 is observed to adjust its channel to 26 as it detects the strong interference from mobile jammers operating in the same channel. Subsequently, WBSN2

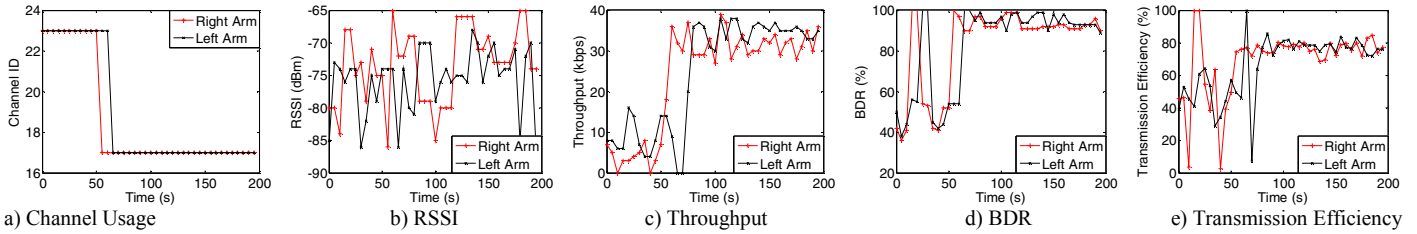


Figure 7 Performance improvement of WBSN5 after channel hopping.

and WBSN3 are both activated at Channel 23. It is observed that WBSN2 does not change its channel during the experiment, while WBSN3 adjusts its channel to 14 after a while. As the mobile jammers and observed users move randomly in the meeting room, the encountered severity of interference may be different at each WBSN user. As such, a WBSN may not switch its channel when its detected interference is still within the tolerable level. After WBSN4 and WBSN5 are activated in Channel 23, they are observed to adjust their channels to 26 and 17, respectively, after they detect heavy utilization in channel 23.

Table I Recorded channel usage in experiment.

	0~2mins	2~4mins	4~6mins	6~8mins
Static jammers(1~3)	12	12	12	12
Static jammers(1~3)	18	18	18	18
Static jammers(1~3)	24	24	24	24
Human jammers(1~3)	23	23	23	23
WBSN1	23	26	26	26
WBSN2	-	23	23	23
WBSN3	-	23	14	14
WBSN4	-	-	23	26
WBSN5	-	-	23	17

The performance results are recorded in the flash memory of each WBSN device. Due to the space limit and the similarity, we only present the performance metrics of WBSN5, shown in Figure 7. From the record, WBSN5 adjusts its channel at the time of 50 s, to avoid severe interference in Channel 23. The RSSIs of the two links in WBSN5 are always greater than -86 dBm and do not show significant difference before and after channel hopping. Such an observation confirms our earlier finding that interference does not have obvious impact on link quality.

From our benchmark study with two transmitters in a network, the individual throughput for each transmitter can reach 40 Kbps on the condition of perfect channels and without external interference. When WBSN5 just starts, the individual throughput of the two transmitters is only around 10 Kbps, 25% of the perfect condition, due to the severe interference from jammers. After hopping to Channel 17, the individual throughput increases to around 35 Kbps, close to the benchmark result (see Figure 7 (c)). As shown in Figure 7 (d), BDR increases from level of 50% to 90%, which significantly increases transmission opportunities for a node. As shown in Figure 7 (e), the Transmission Efficiency is also significantly increased, from level of 50% to 80% when channel hopping is conducted. As a result, the throughput and energy efficiency are significantly improved.

In summary, the experimental results verify the effectiveness of the proposed interference detection and mitigation scheme through channel hopping, and demonstrate that data throughput, BDR, and transmission efficiency are significantly improved in the severely interfered environment.

VI. CONCLUSION

In this paper, we proposed lightweight and robust schemes for interference detection and mitigation in WBSN, to address the problem of performance degradation caused by inter-user interference. From the measurement results, we first identified the suitable performance metrics to be used in detecting the severity of interference in a robust way without any additional energy consumption. We then presented a distributed method to conduct dynamic channel hopping to avoid heavy interference. Our proposed schemes was verified through extensive experiments and proved its effectiveness and performance improvement.

REFERENCES

- [1] S. C. Liu, G. L. Xing, H. W. Zhang, J. P. Wang, J. Huang, S. Mao, and L. S. Huang, "Passive interference measurement in Wireless Sensor Networks", in *Proc. IEEE ICNP*, Kyoto, Page(s): 52 – 61, Oct. 2010.
- [2] D. J. Son, B. Krishnamachari, and J. Heidemann, "Experimental study of the effects of transmission power control and blacklisting in wireless sensor networks", in *Proc. IEEE SECON*, Page(s): 289 – 298, Oct. 2004.
- [3] Suk-Un Yoon, R. Murawski, E. Ekici and P. Sangjoon "Adaptive Channel Hopping for Interference Robust Wireless Sensor Networks", in *Proc. IEEE ICC*, Cape Town, Page(s): 1-5, Dec. 2009.
- [4] D. Peng and G. Roussos, "Adaptive channel hopping for wireless sensor networks", in *Proc. International Conference on Mobile and Wireless Networking*, Shanghai, Pages(s):19-23, Oct. 2011.
- [5] Bin Cao, Yu Ge, Chee Wee Kim, Gang Feng, Hwee Pink Tan, and Yun Li, "An Experimental Study for Inter-User Interference Mitigation in Wireless Body Sensor Networks", *IEEE Sensors Journal*, Volume 13, Number 10, page(s): 3585 – 3595, Oct. 2013.
- [6] Buddhika de Silva, Anirudh Natarajan and Mehul Motani, "Inter-User Interference in Body Sensor Networks: Preliminary Investigation and an Infrastructure-Based Solution", in *Proc. of Body Sensor Networks 2009*, Jun. 2009.
- [7] Wen Sun, Yu Ge and Wai-Choong Wong, "Inter-user Interference in Body Sensor Networks: A Case Study in Moderate-scale Deployment in Hospital Environment", in *Proc. of IEEE HealthCom 2012*, pp.447 – 450, October 2012.
- [8] Wen Sun, Yu Ge, and Wai-Choong Wong, "A lightweight distributed scheme for mitigating inter-user interference in body sensor networks", *Computer Networks (Elsevier)*, Volume 57, Number 18, page(s): 3885-3896, Dec. 2013.
- [9] Yu Ge, Jeng Wai Kwan, Jaya Shankar P., Zhengye Di, Terence S. P. See, Chee Wee Kim, Tat Meng Chiam, and Maode Ma, "Performance Benchmarking for Wireless Body Area Networks at 2.4 GHz", in *Proc. of IEEE PIMRC 2011*, Page(s): 2259-2263, Sep 2011.