Adaptive Interference-Aware Multi-Channel Clustering Algorithm in a ZigBee Network in the Presence of WLAN Interference

Min Suk Kang*, Jo Woon Chong*, Hyesun Hyun*, Su Min Kim*, Byoung Hoon Jung*, and Dan Keun Sung*

*Dept. of EECS, Korea Advanced Institute of Science and Technology
373-1, Guseong-dong, Yuseong-gu, Daejeon, 305-701, KOREA
Phone: +82-42-869-3439,5439
Email: mskang@cnr.kaist.ac.kr, dksung@ee.kaist.ac.kr

***Abstract*— In ubiquitous networking environments, we generally need two or more heterogeneous communication systems coexisting in a single place. Especially, wireless local area networks (WLANs) based on IEEE 802.11 specifications and wireless personal area networks (WPANs) based on IEEE 802.15.4b or g specifications need to coexist in the same Industrial, Science and Medial (ISM) band. If the WPAN communication coverage is expanded using a cluster-tree network topology, then the 802.15.4 network is more susceptible to interference from neighboring WLANs. In this paper, we propose an adaptive interference-aware clustering algorithm using multiple channels in a WPAN in the presence of WLAN interference. The algorithm includes interference detection and avoidance schemes to adaptively reconfigure multiple channels in an IEEE 802.15.4 cluster-tree network to avoid interference from WLANs. To evaluate the performance of the proposed algorithm, the frame error rate (FER) is measured in a real network testbed. The measurement result shows that the proposed algorithm is effective in an IEEE 802.15.4 cluster-tree network in the presence of multiple IEEE 802.11 interferers.**

I. Introduction

Ubiquitous networking enables many objects or devices to be connected and communicate with each other. Wireless local area networks (WLANs) based on IEEE 802.11b or g [1] and wireless personal area networks (WPANs) based on IEEE 802.15.4 [2] can play an important role in future ubiquitous networks. Both networks share the same 2.4 GHz Industrial, Scientific and Medial (ISM) band.

Interference avoidance between IEEE 802.15.4 and IEEE 802.11 has been studied since IEEE 802.11 APs were widely implemented and IEEE 802.15.4 became popular. The interference and coexistence problems between Bluetooth and WLAN devices have been studied [3] - [7].

Especially, a coexistence problem between IEEE 802.15.4 and IEEE 802.11 has been studied recently. Kim et al. [8] evaluated the effect of interference from one IEEE 802.11 AP to one IEEE 802.15.4 link and suggested a scheme for IEEE 802.15.4 devices to adaptively avoid the interference. However, it cannot be applied to a cluster-based IEEE 802.15.4 network with a large number of nodes because it only considers one link environment. Won et al. [9] proposed an adaptive interference avoidance scheme to solve a coexistence problem in a network level when an IEEE 802.15.4 network has multiple devices in a mesh topology. However, this scheme assumes that neighboring devices can still communicate even after the devices are under interference from one IEEE 802.11 AP. Pollin et al. [10] proposed several schemes for selecting a new channel in a distributed cognitive coexistence environment of IEEE 802.15.4 and IEEE 802.11 after detecting interference. However, they are based on a random frequency selection scheme and it is very hard for a group of adjacent devices to move to the same next channel after detecting interference using a random frequency selection scheme.

In this paper, we propose an adaptive interference avoidance algorithm for IEEE 802.15.4 cluster-tree networks. We consider a cluster as a basic group of devices that uses the same frequency channel. Devices do not need to exchange information about which channel they need to move to after detecting interference; each device moves to the next channel which is given from a pseudo random sequence generator whose keys are shared by all devices which use the same channel. This distributed, pre-determined channel change scheme enables IEEE 802.15.4 networks to avoid interference and reconfigure a new cluster-tree network.

The rest of this paper is as follows. In Section II, we describe mutual interference between IEEE 802.15.4 and IEEE 802.11, and introduce an IEEE 802.15.4 based cluster-tree network. In Section III, we propose an adaptive interference-aware clustering algorithm. In Section IV, we introduce an experimental network testbed to evaluate the proposed algorithm. In Section V, we evaluate the performance of the proposed algorithm in terms of frame error rate in an IEEE 802.15.4 cluster-tree network. Finally, we present conclusions in Section VI.

II. ZigBee network and Interference

Figure 1 shows the operational frequency spectrum of both ZigBee and WLAN networks. A WLAN system has eleven

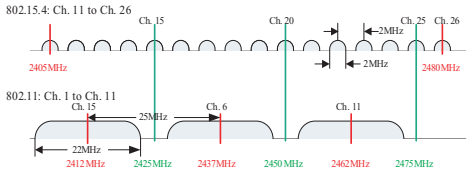

Fig. 1. Frequency Spectrum of ZigBee and WLAN Networks

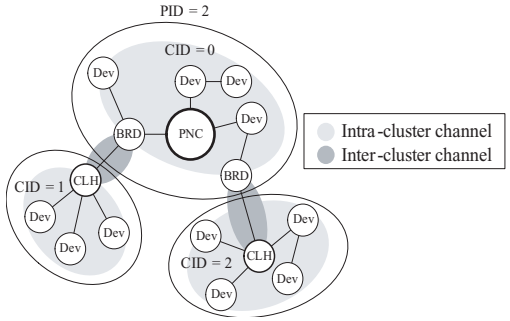

Fig. 2. Example of a ZigBee Cluster-tree Network with Intra- and Inter-Cluster ZigBee Channels

channels. Each channel occupies 22 MHz and up to 3 separate channels can be simultaneously used without any mutual interference. Channels 1, 6, and 11 can be used for neighboring IEEE 802.11 WLAN Access Points (APs), as shown in Figure 1, to mitigate the interference. On the other hand, ZigBee networks have sixteen channels in 2.4 GHz band which can be used simultaneously without any mutual interference among them. Since the transmission power of WLAN is usually 100 times larger than that of ZigBee networks, we focus on the effect of interference from WLAN to ZigBee [1], [2].

The IEEE 802.15.4 WPAN specification describes three topologies: star, peer-to-peer, and cluster-tree topologies. In a PAN, there must be one PAN coordinator (PNC) and it is the primary controller of the PAN. Each independent PAN has a unique identifier, called the PAN id (PID). Figure 2 shows a general network topology with a cluster-tree network. In the cluster-tree topology, devices are grouped by a cluster and a cluster head (CLH), a local coordinator in the cluster, is responsible for managing the cluster and the cluster identifier (CID) is the shared ID number for all devices in the cluster [2]. The cluster-tree network is widely used to increase the coverage area of the ZigBee network using a multi-cluster structure. We define a *bridge device* (BRD), which is a node that is directly connected to a cluster head of a neighboring cluster.

As shown in Figure 2, we define two types of ZigBee channels: *intra-cluster channel* and *inter-cluster channel*. An intra-cluster channel is a channel established by devices in a single cluster and an inter-cluster channel is a channel established by a CLH of one cluster and a BRD of another cluster.

The *same channel group* is defined as a group of devices that share the same channel information and use the same channel. A cluster or a pair of a CLH and BRD can be an example of the same channel group in a cluster-tree network.

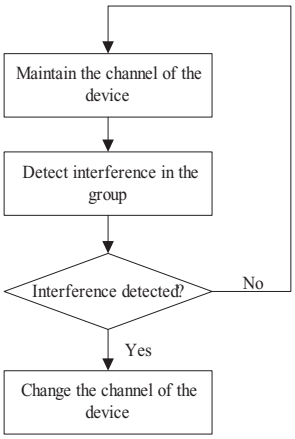

Fig. 3. Simplified flowchart of the proposed algorithm

Under these definitions, CLHs and BRDs belong to two or more same channel groups.

For simplicity we assume a stationary network. In other words, no mobile nodes in the network and no topology changes are allowed. Also, graceful disassociations defined in IEEE 802.15.4 spec. [2] are assumed so that devices do not confuse the disassociation of other devices with interference.

III. Adaptive Interference-Aware Multi-Channel Clustering Algorithm

We propose an adaptive interference-aware multi-channel clustering algorithm for a ZigBee network. Interference is avoided by adaptively changing the channel carrier frequency of ZigBee nodes in the presence of WLAN interference. The algorithm consists of two procedures: an interference detecting procedure and an interference avoiding procedure. Figure 3 shows the simplified flowchart for the proposed algorithm. The first part of the algorithm is an interference detection scheme in which the same channel group detects interference imposed within the group. The second part is an interference avoidance scheme in which the group smartly avoids the interference in the group and reconfigures channels if needed. Algorithms for intra- and inter-cluster channel rearrangements should be applied in different ways. At the end of the section we present how the two schemes can be applied in each case.

A. Interference detection scheme

In IEEE 802.15.4 networks, efficient interference detection with low false alarm probability is very important. Since interference is one of the most serious obstacles for wireless sensor networks, many interference detection schemes have been studied. Zhou [11] suggested an effective radio interference detection (RID) algorithm to detect interference in a sensor network. An interfering node sends test frames to an interfered node. Using the RID algorithm, nodes detect interference. However, we cannot apply this algorithm because we consider interference from another communication system, IEEE 802.11.

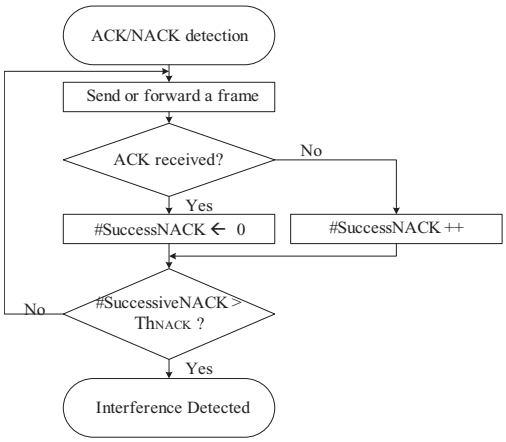

Fig. 4. ACK/NACK based interference detection scheme

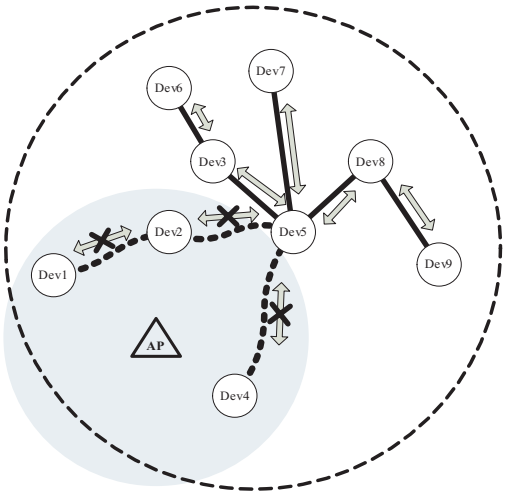

Fig. 5. Interference in a same channel group

Won et al. [9] suggested that an energy detection (ED) scan which uses a RSSI (Received Signal Strength Indicator) value from IEEE 802.15.4 PHY is used to detect interference because the RSSI measurement above a threshold is considered as interference. However, it is known that the RSSI values of IEEE 802.15.4 frames at the distance within 0.3m are almost as high as 250 [12]. Since the RSSI values from near IEEE 802.15.4 devices almost reach its maximum values, 255, it is very hard to set a threshold to filter out interference. Using an ED scan for detecting interference, if a new device that wants to joint the existing PAN is located near one of the existing nodes, the existing node detects interference because the RSSI value from the new node can be almost as high as the maximum RSSI value. Thus, the RSSI-based interference detection scheme is not suitable for IEEE 802.15.4 networks.

Kim [8] presented an *ACK/NACK based interference detection scheme*. Since this scheme does not require redundant procedures for detecting interference, it is the most suitable for cluster-tree networks. Figure 4 shows the flowchart of the scheme. After a sender transmits a frame, it waits for the ACK frame from its recipient. When the sender cannot receive the ACK frame within a timer value, it reports NACK for this transmission. Whenever NACK is reported, it counts up the variable $\#SuccessiveNACK$ by 1. When $\#SuccessiveNACK$ becomes greater than the threshold Th_{NACK}, the sender finds that it suffers from interference.

In a beacon-enabled cluster-tree network, we can use beacon frames to detect interference. The basic concept of the *beacon-based interference detection scheme* is similar to the procedure of ACK/NACK based interference detection scheme. All devices, except the CLH and PNC, receive beacon frames at the beginning of each superframe [2]. When the number of successive lost beacons is greater than the threshold Th_{BF}, the devices finds that they suffer from interference.

For important communication links, such as a link between a CLH and BRD, devices can send and receive *test frames* regularly to examine the link status more often and reliably. In case of these links, the devices can use a *test frame-based interference detection scheme* to detect interference. When a device which is supposed to receive test frames regularly cannot receive them successively, it finds that it suffers from interference.

Since all devices in the group use the same frequency channel, they have to detect and avoid the interference in the group at the same time. If only some part of devices in the group detect and avoid the interference by changing their frequency channel, other devices which cannot detect the interference can remain in the previous channel.

In previous work, various schemes to detect interference to form a group were suggested. Won [9] uses a *Group Formation (GF)* message to form a group of devices which experience interference and need to change their channel to avoid it. The problem is that it is highly likely that devices in the range of interferers cannot listen to the GF message because of strong interference. To avoid this problem, we apply all three interference detection schemes to all devices in a cluster-tree network.

We assume that IEEE 802.11 interference is imposed to the ZigBee channel group. Figure 5 shows an example of the ZigBee channel group consisting of nine devices using the same ZigBee channel. The ACK/NACK-based, the beacon-based, and the test frame-based, interference detection schemes are applied according to the role of each device. Every device that is in the range of the interference of IEEE 802.11 AP can detect the interference directly. However, there could be some devices (Dev3, Dev5, Dev6, Dev7, Dev8, and Dev9) in the group that cannot detect the interference directly. Each device that directly detects the interference transmits a *Channel Change Broadcast Message (CCBM)* to its neighbors so that the remaining devices can detect the interference. Since they are outside of the range of the interference, the remaining devices can receive the CCBM frames. Therefore, using the distributed interference detection schemes and CCBM transmissions, all devices in the same channel group can detect the interference.

B. Interference avoidance scheme

Once a device detects interference within the same channel group or receives a CCBM frame, it now starts to change

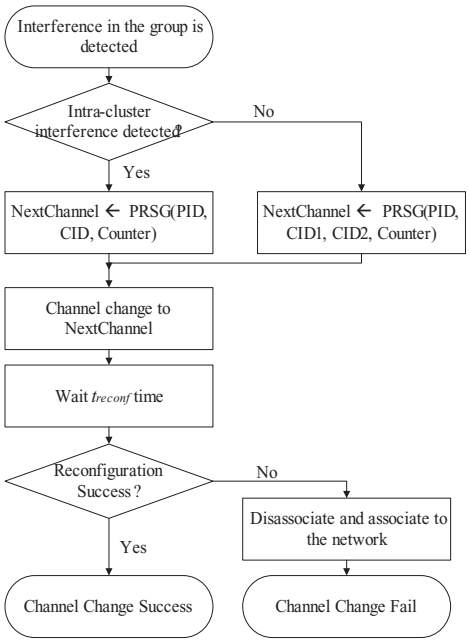

Fig. 6. Flowchart of the proposed Interference Avoidance Scheme

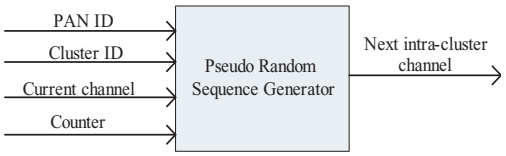

Fig. 7. The block diagram for a Pseudorandom Sequence Generator

its channel to a new channel using an *pseudorandom-based interference avoidance scheme*. Figure 6 shows the flowchart. Each device should have the same next channel sequence so that all the devices move to the same channel after avoiding the interference. In the proposed scheme, ZigBee devices in the group do not need to exchange the next channel information. All the ZigBee devices in the group have a unique key: the combination of their PAN identification (PID) and cluster identification (CID). The combination of PID, CID of CLH, and CID of BRD can be a key for the same channel group consisting of a CLH and BRD. Using this unique key, all the nodes in the group can obtain their shared next channel change sequence from a *pseudorandom sequence generator (PRSG)*, as shown in Figure 7, so that each node does not need to exchange the next channel information with its neighbors.

Nevertheless, there is still some probability that the next channel of the group is interfered by another interferer. In this case, we can add another scheme to check the availability of the next channel before a node changes its channel. To evaluate the availability of the next channel ED scans can be used. If the return value of the ED scan on the next channel shows that the next channel is not used temporarily, then the node is aware that changing channel would be successful. However, when the return value of the ED scan shows that the next channel is busy, the node can increase the counter by one and obtains another channel from the PRSG. Using this scheme, the node can

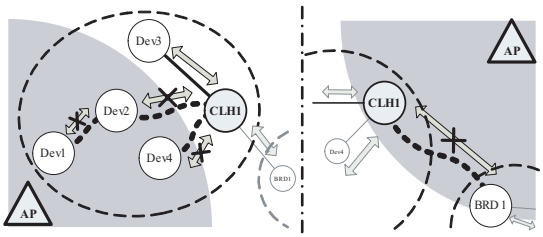

Fig. 8. WLAN Interference in an intra- and inter cluster channel

be aware that the next channel is interference-free. However, this scheme can cause different devices in the group to have different channels. Thus, we suggest a pseudorandom-based interference avoidance scheme without an ED scan.

After moving to the next channel, the node waits for a network reconfiguration period t_{reconf} so that the other nodes can move to the new channel. The device finds that it fails in changing a channel when it cannot find its neighbors after t_{reconf}. Then, all devices, except the CLH and PNC, disassociate from the network and associate it again. When the node attempts an association again, it starts from Passive Scan [2] to join the network. Through the Passive Scan it now finds which channel it should use to communicate with the network. If the device is CLH or PNC, it performs the interference detection scheme and the interference avoidance scheme again to change its channel to another one.

C. Algorithm for an Intra-cluster channel

The left-hand side of Figure 8 shows a typical example of interference within a cluster. In this case, the cluster is the same channel group. A WLAN AP channel provides interference to the ZigBee channel used in the cluster. Three ZigBee devices (Dev1, Dev2, and Dev4) are within the communication coverage of the WLAN AP.

Each node, except the CLH, can determine whether it experiences interference by using the ACK/NACK-based and Beacon-based interference detection schemes at the same time. If the node is a CLH, then it only uses the ACK/NACK-based interference detection scheme to detect interference in the cluster.

If the node detects the interference, it then sends a CCBM frame and obtains the next channel using its PID and CID. Then it waits t_{reconf} for reconfiguration.

D. Algorithm for an Inter-cluster channel

The right-hand side of Figure 8 shows a typical example of interference on WLAN inter-cluster channels. In this case, only two devices, the CLH and BRD, belong to the same channel group. Both of the CLH and BRD, or one of them can experience the interference. Inter-cluster channels need to be treated with greater care, compared with intra-cluster channels, because the performance may degrade more severely if they are interfered by WLAN APs.

For more robustness on the inter-cluster channels, CLHs send periodic test frames to their BRDs. The CLH easily detects whether its inter-cluster channel experiences interference using the ACK/NACK-based interference detection scheme.

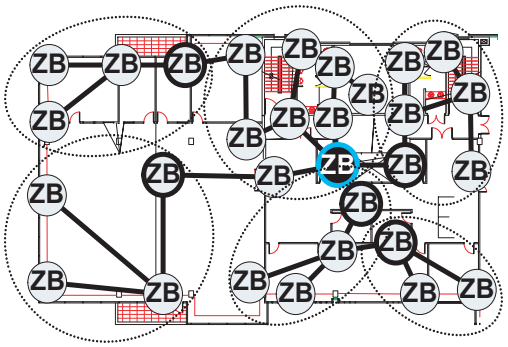

Fig. 9. Cluster-tree network in the testbed

ACK frames are sent from the BRD corresponding to data frames or test frames sent from the CLH. The BRD can detect the interference using the test frame-based interference detection scheme.

After detecting interference, devices send a CCBM frame and obtain the next channel using their PID, CID1 (CID of CLH), and CID2 (CID of BRD). Then, they wait t_{reconf} for reconfiguration.

IV. Experimental Environment

To verify the proposed algorithm, we perform some experiments in a network testbed.

A. Testbed

The network testbed consists of 30 ZigBee nodes and 6 WLAN APs. Figure 9 shows the placement of the ZigBee nodes and WLAN APs in an indoor environment. The ZigBee network is implemented using Crossbow's MICAz motes which are IEEE 802.15.4 compatible and uses Chipcon's CC2420 chip and ATMel's ATMega128. The MICAz mote is running on TinyOS and written by NesC. The WLAN APs are NETGEAR's WG302 APs which support IEEE 802.11b/g.

The ZigBee cluster-tree network is configured and clusters are formed, as shown in Figure 9. The ZigBee device named PNC is the PAN coordinator, and the devices with the name CLH indicate the cluster heads. We divide the clusters regardless of the positions of WLAN APs in order to model real scenarios. When we apply the proposed algorithms, cluster heads and bridge nodes work as multi-channel devices.

B. Traffic Setup

We set each data payload size to 10 bytes, and, thus, the total length of PHY protocol data unit (PPDU) is 51 bytes. For the ZigBee network, the transmit power strength is set to its maximum. Every node, including the PAN coordinator, generates and sends a data frame at constant bit rate (CBR), because IEEE 802.15.4 networks are used as sensor networks whose nodes send sensor data regularly to their PAN coordinator. Ack frames are required for all ZigBee frames and beacons are not used. In other words, the network is operated in non-beacon mode.

WLAN APs communicate with laptops which download a large amount of files from a server using FTP protocol. When an AP transmits FTP data frames, it occupies the frequency spectrum with a high channel usage and it causes steady interference to the ZigBee network. We set the transmit power level of the WLAN APs to minimum in order to minimize the coverage area of each WLAN AP. For simplicity, we use only channels 1, 6, and 11, and set the channel number of each AP, as shown in table I.

TABLE I
Allocation of WLAN AP Channels

IEEE 802.11 WLAN AP	IEEE 802.11 channel
AP1	channel 11
AP2	channel 1
AP3	channel 11
AP4	channel 6
AP5	channel 1
AP6	channel 11

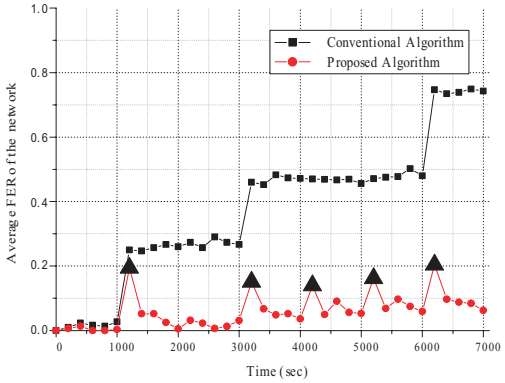

Fig. 10. FER Performance

V. Experimental Result

To investigate the effect of IEEE 802.11 WLAN devices over IEEE 802.15.4 WPAN network, measurements were made in the actual network testbed descridbed in Section IV.

We observe how the frame error rate (FER) performance of the network varies over time. The FER values are gathered every 200 seconds. We turn on IEEE 802.11 WLAN APs one by one for every 1000 seconds. We observe how the proposed algorithm manages the operating channel of each cluster whenever new interference appears.

The FER is calculated as follows:

$$FER = \frac{\#\ of\ received\ frames\ at\ PNC\ under\ interference}{\#\ of\ received\ frames\ at\ PNC\ in\ ideal\ case}.$$

A. Frame Error Rate of the conventional cluster-tree network

As shown in Figure 10, we first observe the FER curve for the conventional ZigBee cluster-tree network. At first, all the devices in the network are set to operate on the ZigBee channel 23 and there is no active WLAN AP on the same floor. In the interference-free environment, the FER value is about 0.045. The non-zero FER values indicate that the network is set in an indoor environment with many walls, walking people, and other interferers.

When AP#1 is turned on, approximately 1/3 of devices in the network are not able to communicate. For AP#2, we cannot find any performance degradation because the channel of AP#2 is not on the same frequency spectrum as that of the ZigBee network (channel 23). AP#3 and AP#6 are using WLAN channel 11 which affects ZigBee channels 21, 22, 23, and 24. (As shown in Figure 1 and Table 1) Thus, only AP#3 and AP#6 increase the FER of the system; the other APs do not affect the FER of the system. After all, all the APs are turned on, the FER values are almost 1, which implies the network is almost incapable of communication.

B. Frame Error Rate of the proposed cluster-tree network

Second, we observe the FER performance of the proposed algorithm in the same interference environment. When AP#1 is turned on, the FER of the network is increased up to 0.22. The FER of the proposed network during the first 200 seconds after AP#1 is on is lower than for the conventional network. Since intra- or inter-cluster channels under interference from WLAN APs are changed to new channels and the network reconfiguration is processed for the new channels within 200 seconds. The network shows only a short-term performance degradation (triangle marks in Figure 10) during this transient period. After the network starts to suffer from new interference, the performance of the network is almost recovered within 200 seconds. There is a short-term performance degradation after AP#3 and AP#6 are on, as discussed in the case for the conventional network.

Note that there is no performance degradation after AP#2 is on because there is no interference from AP#2. However, there are small degradations after AP#4 and AP#5 are power-on. This phenomenon is due to the widely distributed channels of the network. When an interfering WLAN AP is turned on, some channels of the ZigBee network are changed. Thus, after AP#1 and AP#3 are turned on, channels used in the network are not homogeneous, but highly distributed. When AP#4 and AP#5, which use WLAN channel 6 and channel 1, respectively, are turned on, some parts of the network have already used the same ZigBee channels which are interfered by WLAN channels 6 and 11 and they change their channels to the next ones. However, the network recovers its performance by the proposed algorithm during a short period.

Despite of success in interference mitigation, the proposed algorithm does not resolve the overall FER degradation of the network as the number of WLAN APs increases. The reason is that the increasing number of *edge devices* degrades the overall performance of the network. The edge devices are the ZigBee devices which are located in the edge of the coverage area of WLAN APs. In the edge, the interference from the WLAN AP is not strong enough to let the devices detect that they are under the interference of the WLAN AP; however, the edge devices sometimes lose frames or receive frames with errors, and, thus, the performance is degraded.

VI. Conclusions

IEEE 802.15.4 ZigBee networks have been widely deployed, coexisting with heterogeneous systems, such as WLAN or Bluetooth. The coverage area of the ZigBee network is generally rather large and the ZigBee network is more prone to experiencing interference from neighboring interferences like WLAN APs.

In this paper, we propose an adaptive interference-aware multi-channel clustering algorithm for a ZigBee cluster-tree network. In the proposed algorithm, two types of channels are reconfigured under the severe interference from WLAN APs. The channel used within a cluster, called an intra-cluster channel, is selected and managed by the cluster head (CLH) of the cluster. The channel used to connect two different clusters, called an inter-cluster channel, is selected and managed by the cluster head (CLH) from one cluster and the bridge node (BRD) from another cluster. We propose five effective and feasible algorithms to detect the interference and avoid it. The measurement results in the real network testbed show that the proposed algorithm is more effective in the real cluster-tree ZigBee network in the presence of interference from multiple WLAN APs.

Acknowledgment

This study has been supported in part by a grant (Next Generation PC Project) from the Institute of Information Technology Assessment (IITA)

References

[1] IEEE 802.11b Specification, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band*, Sep. 16, 1999.

[2] IEEE 802.15.4 Specification, *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)*, Oct. 1, 2003.

[3] J.-H. Jo, H. Jayant, "Performance evaluation of multiple IEEE 802.11b WLAN stations in the presence of Bluetooth radio interference," *ICC 2003*, Vol. 2, pp. 1163 - 1168, May 2003.

[4] W. Feng, N. Arumugam, G. H. Krishna, "Performance of a Bluetooth piconet in the presence of IEEE 802.11 WLANs," *PIMRC 2002*, Vol. 4, pp. 1742 - 1746, Sept. 2002.

[5] I. Sakal, D. Simunic, "Simulation of interference between Bluetooth and 802.11b systems," *EMC 2003*, Vol. 2, pp. 1321 - 1324, May 2003.

[6] I. Howitt, "WLAN and WPAN coexistence in UL band," *IEEE Trans. of Veh. Tech.*, Vol. 50, No. 4, pp. 1114 - 1124, July 2001.

[7] W. Feng, N. Arumugam, G. H. Krishna, "Impact of interference on a Bluetooth network in the 2.4 GHz ISM band," *ICCS 2002*, Vol. 2, pp. 820 - 823, Nov. 2002.

[8] S. M. Kim, J. W. Chong, C. Y. Jung, T. H. Jeon, J. H. Park, Y. J. Kang, S. H. Jeong, M. J. Kim, and D. K. Sung, "Experiments on Interference and Coexistence between Zigbee and WLAN Devices Operating in the 2.4 GHz ISM Band," in *Proc. NGPC*, pp. 15 - 19, Nov 2005.

[9] C. Won, et al., "Adaptive Radio Channel Allocation for Supporting Coexistence of 802.15.4 and 802.11b," in *Proc. VTC*, Vol. 4, pp. 2522 - 2526, Sep 2005.

[10] S. Pollin, et al., "Distributed cognitive coexistence of 802.15.4 with 802.11," in *Proc. Crowncom*, 2006.

[11] G. Zhou, T. He, J. A. Stankovic, T. Abdelzaher, "RID: radio interference detection in wireless sensor networks," in *INFOCOM 2005*, Vol. 2, pp. 891 - 901, Mar 2005.

[12] S. W. Kong, T. H. Jeon, S. J. Kim, J. W. Chong, M. S. Kang, S. M. Kim, C. Y. Jung, and D. K. Sung, "A ZigBee-Based Centralized Location Tracking System for Reducing the Locationing Traffic Load", *NGPC*, 2007.