Facilitating Non-Collocated Coexistence for WiFi and 4G Wireless Networks

Punit Rathod
Department of CSE
Indian Institute of Technology Bombay
Powai, Mumbai - 400 076
Email: punit@cse.iitb.ac.in

Abhay Karandikar
Department of Electrical Engineering
Indian Institute of Technology Bombay
Powai, Mumbai - 400 076
Email: karandi@ee.iitb.ac.in

Anirudha Sahoo
Department of CSE
Indian Institute of Technology Bombay
Powai, Mumbai - 400 076
Email: sahoo@cse.iitb.ac.in

***Abstract*—In this paper, we discuss the problem of non-collocated coexistence of WiFi and 4G technologies such as WiMAX and LTE due to adjacent channel interference. The existing literature has many solutions and schemes to address the problem of shared channel coexistence and adjacent channel coexistence on multi-radio platforms. Results for Non-collocated coexistence in adjacent channels in wireless remain very scattered and few. Radio devices operating on Broadband Wireless Access (BWA) 4G wireless technologies like IEEE 802.16 (WiMAX) and LTE-A require very low noise floor. BWA spectrum allocations in 2.3 GHz and 2.5GHz have resulted in these networks to be very close to 2.4 GHz ISM band used by WiFi. We show, with measurements on our test-bed and from existing results, that the low-cost filters on WiFi devices are not very effective in controlling the out-of-band emissions to satisfy the low noise floor requirements of 4G. We propose schemes to mitigate the problem of adjacent channel interference by a time sharing mechanism across technologies by protecting packet receptions on both IEEE 802.11 and the IEEE 802.16 side. We demonstrate the effectiveness of our scheme to protect WiMAX packets by ensuring a controlled silence zone in the WiFi network using a test-bed. We also show that there is very limited adverse impact, due to the use of our scheme, on the system throughput of the non-collocated WiFi network operating in the adjacent channel.**

I. Introduction

Wireless broadband networks aim to provide very high data rates to users at distances upto 5 km. Significant amount of research effort is directed towards optimizing the spectrum efficiency of wireless technologies to extract the maximum possible throughput from the minimum possible spectrum. However, spectrum is a limited natural resource and many wireless technologies are being packed close to each other in adjacent channel bands. The allocations for 4G technologies such as WiMAX and LTE in India include the 2.3 GHz and 2.5 GHz bands [1] . These frequencies are adjacent to the unlicensed 2.4 GHz ISM band and a cause of concern that we explore in this paper.

In the specific case of India, the frequencies alloted to 4G wireless broadband technologies — broadband wireless access (BWA) are in the 2.3 GHz band [1]. The frequency allocations in the 2.3 GHz bands are as close as 2340 MHz to 2400 MHz in certain cases. The 2.4 GHz ISM band is very densely populated with IEEE 802.11 WiFi devices and Bluetooth devices. IEEE 802.11 a/b/g devices are known to cause interference in both overlapping channels and adjacent channels [14]. Any signal transmitted outside the legal 20 MHz channel bandwidth of a WiFi channel is an out-of-band signal. The interference in adjacent channels is largely due to poor out-of-band signal rejection of IEEE 802.11. This raises a concern that devices from different technologies may not coexist gracefully even when they do not share the same spectrum. We refer to this situation as non-collocated coexistence in adjacent channels.

With the recent advances in highly portable gadgets like tablets, netbooks, ultrabooks and smartphones, the penetration of WiFi and Bluetooth enabled devices has increased significantly. There is also a major shift in the kind of applications and services that drive the data demands in networks. Online gaming, videos, real-time streaming, social networking have become very popular. In this context, it is very unlikely that the popularity of WiFi will recede after 4G technologies like WiMAX or LTE are deployed. Even from a network planning perspective, WiMAX and LTE network operators would prefer the end user devices to migrate to WiFi when they are indoor and within range of a WiFi hot-spot . This would lead to a situation where there will be a healthy mix of both WiFi and 4G devices coexisting in a given geographical area.

In this paper, we consider WiMAX as the 4G technology that operates on the adjacent channel to WiFi. We propose a solution to mitigate interference from adjacent channels in non-collocated coexistence. The proposed schemes can be extended for other technologies like LTE and LTE-Advanced.

Organization of the paper: Related work is discussed in Section II and the motivation is presented in Section III. We discuss the System Model used in our work in Section IV. In Section V, we discuss the schemes to mitigate the interference due to non-collocated devices operating in adjacent channels. Section VI discusses the experimental setup and the initial results for protecting transmissions in non-collocated coexistence scenario. In Section VII, we discuss improvements to the scheme with transmit power control. Concluding remarks and future work are discussed in Section VIII.

II. Related Work

The related literature can be broadly classified into collocated coexistence and non-collocated coexistence mitiga-

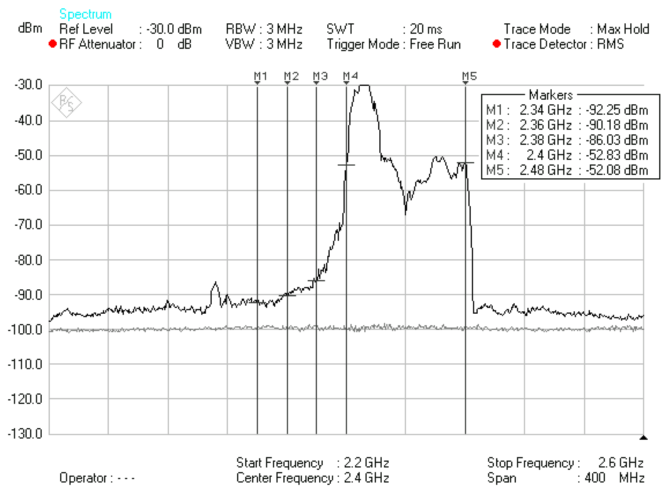

Fig. 1. Spectrum scan in the Information Networks Lab, Department of Electrical Engineering, IIT Bombay.

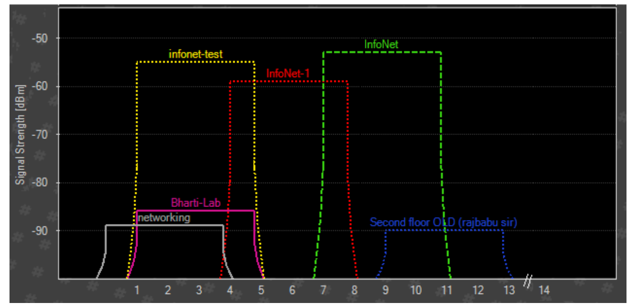

Fig. 2. Active access points monitored using inSSIDer the Information Networks Lab, Department of Electrical Engineering, IIT Bombay.

tion schemes. The problem of collocated coexistence across technologies on a multi-radio platform has been studied in [18] [16] and the references therein. Collocation coexistence mainly deals with the coordination across interfaces in a multi-radio platform with a coordination block. The radio interfaces on the multi-radio platform exchange signals through the coordination block to schedule transmissions (either shared channel or adjacent channel).

In the case of non-collocated coexistence, there is further division on the basis of handling shared channel and adjacent channel interference. Non-collocated coexistence across different devices on separate technologies but on the same channel has been studied in [12] [13] [9]. In [12], the authors discuss the impact of non-collocated coexistence when both IEEE 802.11 and IEEE 802.16 devices operate in the same channel. Schemes to mitigate the impact of non-collocated coexistence while operating in the same channel are discussed in [13] and [9].

Non-collocated coexistence of WiFi and Bluetooth falls in the category of both shared channel and adjacent channel coexistence of non-collocated coexistence. This problem has been well studied in the literature. Authors in [6] and the references therein propose methods to mitigate interference across WiFi and Bluetooth devices when they operate, on the same or adjacent channels, within the 2.4GHz Band.

To the best of our knowledge, the issue of non-collocated coexistence, where, the devices operate on adjacent channels has not received much attention. The focus of this paper is to discuss the impact of interference due to adjacent channel interference and propose schemes to mitigate the same.

III. Motivation

IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMAX) [2], is one of the 4G standards that can facilitate the last mile wireless broadband access as an alternative to cable and Digital Subscriber Line (DSL). This last mile wireless is also dominated by very dense deployment of personal and commercial WiFi access networks. WiFi uses a channel width of 22 MHz while operating in IEEE 802.11b mode and 20 MHz while operating in IEEE 802.11g/n mode [3]. The legal channels for WiFi occupy frequencies from 2400 MHz to 2484 MHz in most parts of the world. WiMAX channel bandwidths can be 1.25 MHz, 5 MHz, 10 MHz and 20 MHz depending upon the band used. WiMAX channels are in 2.3 GHz and 2.5 GHz licensed band and the exact frequencies used vary from country to country.

A typical wireless coverage map in our lab (InfoNet lab inside the Department of Electrical Engineering, IIT Bombay) is shown in Figure 2. The channel occupancy of wireless access points is obtained using the inSSIDer wireless analyzer tool [7]. Looking at the central frequency of the envelopes, it can be seen that there are multiple wireless networks occupying most of the orthogonal Channels 1, 6 and 11 (center frequencies 2412 MHz, 2437 MHz and 2462 MHz respectively). It is difficult to avoid channels 1 and 11 and prevent interference with 2.3 GHz and 2.5 GHz BWA networks. We also capture the spectrum utilization of these networks on a hand held spectrum analyzer (Rhode & Schwarz FSH8) to observe the out of band spillage. In Figure 1, we concentrate on the channel occupancy of a wireless network operating on Channel 1 of IEEE 801.11 (2402 MHz to 2422 MHz). It can be seen that the out-of-band signal received from WiFi networks is as high as -86dBm (at 2380 MHz) even at a separation of more than 20 MHz which is out side the 2.4 GHz band — Marker M3 in Figure 1. This is a conservative estimate because the antenna used during the measurements was optimized for operations in the ISM band only (2.4 GHz).

These findings are further strengthened by the observations in [5]. It has been shown by authors in [5] that even at a separation of 114 MHz, WiFi signals can be received with signal strength of -75 dBm. This is largely due to the fact that WiFi devices use low cost filters that are not very efficient in reducing out of band spillage. Authors in [5] report that the WiFi channel at 2.412 GHz (Channel 1) generates out of band spillage of up to -61 dBm which results in an in-band interference for the adjacent 2.380 GHz WiMAX channel. Similarly 2.462 GHz (Channel 11) generates an in-band interference of levels up to -75 dBm for the adjacent 2.576 GHz WiMAX channel. This has also been independently

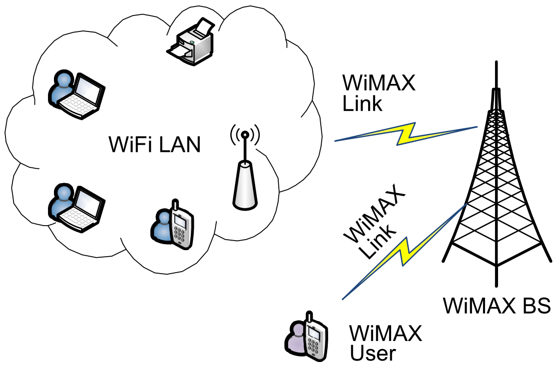

Fig. 3. A WiMAX-WiFi Coexistence Scenario.

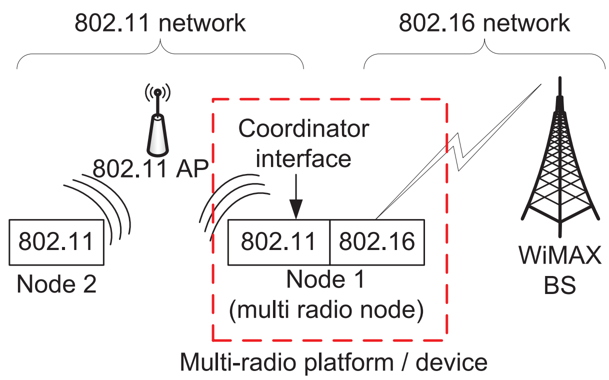

Fig. 4. Coordinator interface and CLC

verified by us (Figure 1).

The WiMAX devices operate with a receiver sensitivity of -114 dBm [2]. Hence, an isolation of 53 dB is required between WiMAX and WiFi antennae in ideal conditions, where there is out of band spillage of upto -61 dBm : $|-114dBm-(-61dBm)| = 53dB$. This corresponds to a free space separation distance of around 7 m. The spectrum analyzer plots also show difference in out of band emissions generated by signal generator and actual WiFi hardware. Authors in [17] also suggest a minimum isolation distance of 7 m or a isolation of 56 dB to 60 dB when WiMAX and WiFi devices are in very close proximity to each other.

IV. System Model

We consider a scenario where a network has both WiFi and WiMAX stations coexisting within close proximity. This includes situations like coffee shop hot-spots, airport hot-spots, home WiFi networks. A local WiFi network enables connectivity to a group of users in the smaller distance range of upto 100 m. The WiMAX network enables connectivity to devices like laptops and mobile phones that are clients in a range of upto 5 km. In such a scenario, some of the WiFi and WiMAX devices may be located close to each other. This could lead to adjacent channel interference causing degradation of performance in both networks as discussed in Section III. A typical network setting is shown in Figure 3.

Collocated interference occurs when one of the radio interfaces is transmitting and another is receiving. The problem of collocated interference can be solved with the help of a simple time sharing method. As in the case of multiple wireless interfaces on a single platform, signaling between the radios can be used to coordinate the transmissions.

TABLE I
Interference matrix for WiFi and WiMAX transmissions

WiMAX \ WiFi	Transmit	Receive
Transmit	No Interference	**Interference**
Receive	**Interference**	No Interference

The interference generated by transmit and receive operations of the WiFi and WiMAX devices is summarized in Table I. When both client devices on different technologies are transmitting, the corresponding receivers are assumed to be reasonably far apart. The WiFi access point is typically located indoors for the hot-spot coverage and the WiMAX base station is typically located outdoors on a tower and hence the corresponding receivers of the client devices are not affected by the adjacent channel interference. Similarly, in the case of adjacent WiFi and WiMAX devices receiving simultaneously, the corresponding transmitters are farther than the 7 m range to the other receiver as highlighted in Section III and hence will not cause any problem. In cases of *WiFi device transmitting* and the *WiMAX device receiving* or *vice-versa*, the adjacent channel interference is a problem. We look at ways to mitigate this interference in the subsequent Sections.

V. Protection for Transmissions

We assume that the Collocated Coexistence (CLC) Controller enabled WiMAX device is a dual radio device with both WiFi and WiMAX radio interfaces. When the WiMAX interface is in use, the spare WiFi radio interface can be used for coordination across users. This coordinator interface will allow arbitration of radio resources across multiple nodes when both WiFi and WiMAX devices are in close proximity to each other. The location of the multi-radio node with respect to the WiFi and WiMAX networks is shown in Figure 4. It is important to note that the WiFi interface of the multi-radio WiFi-WiMAX node is not associated with the WiFi access point and is just within the interference range of a potentially interfering WiFi device. The CLC Controller is a module that exists inside the multi-radio node for coordination across interfaces.

The WiFi interface in the dual-radio device will remain in promiscuous listening mode when WiMAX radio is being used. This will allow the WiFi interface to gather information about interfering nodes in the proximity and decide whether a coordination action has to be undertaken by the CLC Controller. The WiFi interface on the multi-radio platform will be referred to as the coordinator interface hence forth in this paper. As seen in Table I, when both WiFi and WiMAX are transmitting or receiving, there is no problem of adjacent channel interference. The adjacent channel interference exists only in the case of one of the devices transmitting while the other device is receiving.

The coordinator interface listens to the WiFi channel in promiscuous listening mode on channels adjacent to the one being used by WiMAX e.g., if the WiMAX SS is operating on 2380-2400 MHz channel, then Channel 1 of WiFi (2412 MHz) will be monitored and similarly if WiMAX SS is operating on 2496-2516 MHz channel, then Channel 11 of WiFi (2462 MHz) will be monitored. The coordinator interface checks for received power level of packets on the adjacent WiFi channel. If the received power is greater than the interference threshold, then the CLC Controller is informed about the action to be taken in order to protect packet receptions by both WiFi and WiMAX radios.

With the help of CLC Controller and Coordinator interface, we propose a novel scheme where one of the radios among WiFi and WiMAX has to back-off allowing the other device to continue the communication. This helps in mitigating the effects of adjacent channel interference on the transmissions and reception of packets. We deal with both WiFi and WiMAX protection separately. When the WiMAX SS is receiving a packet, we protect the WiMAX packet by inhibiting any WiFi transmission in the interference range. Similarly, when WiFi interface is receiving a packet, we protect the WiFi packet by informing the WiMAX BS to not schedule any transmissions by WiMAX SS. Both the schemes are presented in detail in the subsequent sections.

A. Protecting WiMAX Reception

The fist block in each WiMAX frame contains the schedule provided by the WiMAX BS. This control block containing the schedule is called the MAP. MAP contains both the uplink (UL-MAP) and downlink (DL-MAP) schedule to be followed. By inspecting the DL-MAP, the WiMAX SS is aware of the incoming packets in the current frame. The coordinator interface decides, based on the measurements on adjacent channels, if a WiFi device in the vicinity can potentially interfere. If a WiFi device is found, then CLC Controller is informed about coordinating the transmissions.

In case of WiFi transmissions, the nodes determine the transmit opportunity based on a binary exponential back-off if the WiFi channel is found to be idle. The WiFi protocol provides for various control packets to ensure collision free communication. In our scheme, we exploit the behavior of WiFi nodes in hidden node situations to our advantage. WiFi uses Request-to-Send (RTS) and Clear-to-Send (CTS) packets between source and destination before a packet transmission. Both, RTS and CTS packets contain a Network Allocation Vector (NAV). The NAV indicates the total time required by the source and destination to complete the transmission. All nodes that hear the CTS packet are required to abstain from transmitting packets for a duration specified in the NAV.

Nodes that hear a RTS packets and not the CTS, can still proceed with transmissions — exposed node scenario of WiFi. However, it is mandatory for nodes to back-off all transmissions if they hear a CTS packet — hidden node scenario in WiFi. This behavior of the protocol is used to protect WiMAX SS packet reception.

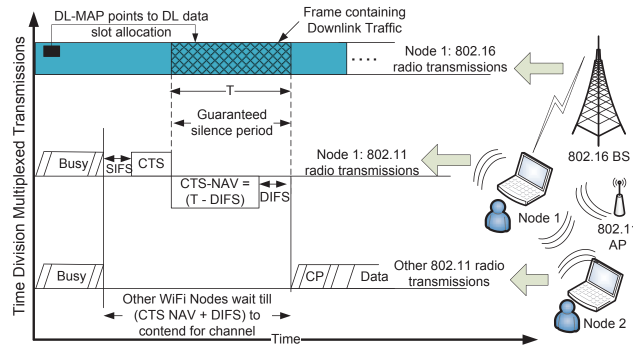

Fig. 5. Protecting WiMAX reception

Figure 5 shows the protection of WiMAX packet reception. The DL-MAP comprising of the downlink schedule points to the WiMAX SS downlink slots in the next frame. The duration of one WiMAX frame is typically 5 ms. Just before the start of the next WiMAX frame, the CLC Controller is informed by the WiMAX interface to generate a CTS packet with NAV equivalent to the WiMAX frame duration. The CLC Controller uses the WiFi coordinator interface to transmit a CTS packet. All WiFi nodes in the vicinity of WiMAX SS that hear the CTS packet abstain from transmitting packets for the duration of the NAV, hence protecting the WiMAX SS packet reception.

B. Protecting WiFi Reception

The WiFi devices receive data and control packets that may be both periodic and aperiodic. Protecting the periodic control packets (like Beacons) is important for reliable functioning of the WiFi network (eg: multiple missed beacons leads to disconnection from the AP). Interference to the WiFi reception could be from nearby WiMAX SS. The WiMAX SS transmit slots are assigned by the WiMAX BS in the UL-MAP. The WiMAX SS does have control over the time slots being used. IEEE 802.16m standard proposes a collocation aware base station scheduler. The IEEE 802.16m standard also provides special control messages for CLC, viz. CLC_Request and CLC_Report. CLC_Request allows a WiMAX SS to inform the WiMAX BS about periodic interference from collocated WiFi devices. The WiMAX BS then uses this information to schedule uplink and downlink slots for the corresponding WiMAX SS so that the SS is not active in interfering time slots. The CLC_Report is a report generated by the WiMAX SS to give information about the collocated interference experienced by the SS. For non-periodic WiFi receptions, currently there is no provision in CLC control messages of WiMAX BS and SS. Non-periodic traffic is harder to protect because of two reasons, (a) prediction of WiFi receive instances is hard, (b) WiMAX transmit schedule is fixed in a centralized manner at the BS, and it is difficult for the WiMAX BS to predict the WiFi receive schedule for the aperiodic traffic.

We use the CLC_Report message to request WiMAX BS to allow priority to periodic WiFi receptions. The CLC_Report

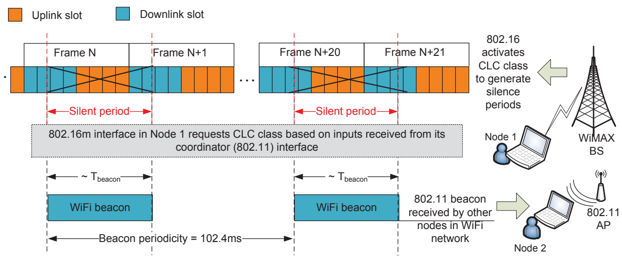

Fig. 6. Protecting WiFi reception

message requires both the duration and periodicity of the WiFi receptions that are to be protected. The duration of WiFi activity to be protected is referred to as the Silence Period. Given both the parameters, the WiMAX BS will ensure that it does not schedule any WiMAX activity for the corresponding WiMAX SS during the silence periods.

Determining the duration and periodicity of WiFi reception on a dual radio device, where both WiFi and WiMAX radios are active, is straightforward. A single control interface between the WiFi and WiMAX radios can pass on the information about channel activity across radio interfaces. However, we consider coordination across multiple devices where radio interfaces are not collocated within the same device. In both Basic mode of operation and DCF mode of operation in WiFi, the receiver WiFi node sends an ACK packet to confirm a successful packet reception. The coordinator interface listens for the ACK packets to determine the distance from the receiver. If received power of ACK packet is greater than -61 dBm as received by the coordinator interface, then the coordinator interface starts measuring periodicity of received packets. Received packets to be protected fall in two categories (a) beacon frames (periodicity of beacon frames is available as a parameter inside the beacon frames). (b) measured receive traffic with a observable periodicity (CBR traffic). The CLC_Request control message is then generated with the measurements generated by the coordinator interface.

Figure 6 shows the channel activity on WiFi and WiMAX nodes when protection is requested for periodic beacons of WiFi. Node 1 in the figure represents a dual radio node with both WiFi and WiMAX interfaces. WiFi interface of Node 1 is also the coordinator interface for CLC. Node 2 in the figure represents a WiFi node. The coordinator interface on Node 1 measures the duration and periodicity of beacon frames received by Node 2 from the WiFi access point. This information is conveyed to the WiMAX BS in a CLC_Request packet. As seen in Figure 6, the WiMAX BS does not schedule any transmissions in the slots marked with 'X' for SS Node 1. This ensures that WiFi reception is protected.

The WiMAX BS can still schedule packet reception on the WiMAX SS during the silence periods because there is no impact on the packets if both WiFi and WiMAX users are receiving at the same time. The coordinator interface also ensures that the CLC_Request is generated only for packet receptions destined for Node 2. This ensures that simultaneous transmission and reception of WiFi and WiMAX is allowed.

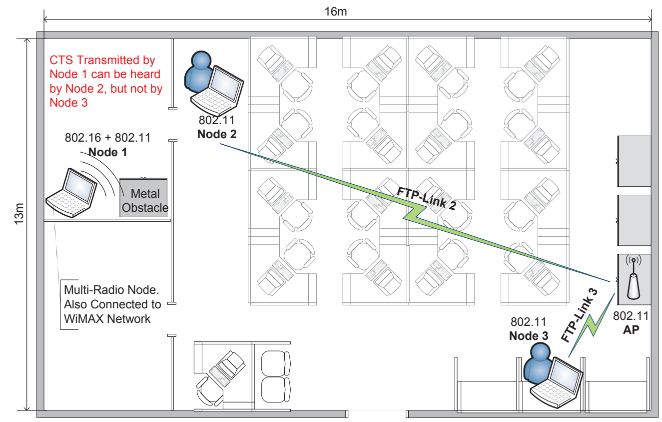

Fig. 7. Experimental Setup inside Information Networks Lab, Department of Electrical Engineering, IIT Bombay

VI. Experimental Evaluation

The proposed schemes consists of two modules, WiMAX protection module and WiFi protection module. The WiMAX protection module sends a CLC_Report to WiMAX BS when there is an interfering WiFi device. The WiFi protection module uses the coordinator interface to send a CTS message to silence the neighboring WiFi devices. Due to unavailability of WiMAX base station for evaluation and testing, we have implemented only the WiFi protection module and emulated the WiMAX behavior. The WiFi protection module assumes a Poisson arrival of incoming packets on the WiMAX SS. Based on these Poisson arrivals, the coordinator interface decides to send a CTS packet with a NAV of 5 ms.

The floor plan of the test-bed is shown in Figure 7. We are concerned with 3 nodes in the testbed labeled Nodes 1 to 3. Node 1 is the dual radio WiFi/WiMAX node, and the WiFi interface of this node is operating in promiscuous listening mode to monitor Channel 1 (2.412 GHz) of WiFi for interfering nodes. Node 2 is at a 3 m distance from Node 1. Node 3 is at a 17 m distance from Node 1 and also separated by a brick partition. Nodes 2 and 3 are connected to an access point that is placed near Node 3. This particular setup shown in Figure 7 is chosen specifically to replicate situations where more than one node is associated to the WiFi access point and not all the WiFi nodes are interfering the WiMAX device.

A. WiFi Implementation

We need to make driver changes only in the dual radio device to enable sending of modified CTS packets. All the other WiFi devices in the network do not need any changes in their drivers and operate with normal WiFi protocol stack.

1) Challenges in Selecting Hardware for Test-Bed: The choice of appropriate hardware for the test-bed was a challenging task. There were multiple factors to be considered for the choice for the wireless card:

Interface on PC (USB, PCI, MiniPCI): MiniPCI interface cards were ruled out as an option because of unavailability of compatible embedded boards. A Desktop based PCI card was a good candidate because of the availability of right chipset and drivers. A USB interface was also preferable because of portability of the USB WiFi dongles.

Full Source Code availability for Drivers: Implementation of our scheme on the coordinator interface required monitor mode support for the wireless interface and ability to patch the drivers to generate packets.

Detachable antenna: In the experimental evaluation, we had to reduce the transmit power to very low levels. Software transmit power control provided by the driver does not allow powers less than 1dBm on most cards. Hence it was essential to use external RF attenuators to reduce the transmit power.

Monitor mode support: One of the key requirements for the coordinator interface is to be able to passively monitor wireless traffic on the adjacent interfering WiFi channel and collect statistics to assist in coexistence coordination. Only select few chipsets support Monitor mode of operation viz: Atheros, Realtek RT8187

Packet Injection: A key requirement of the coordinator interface is to be able to generate CTS packets with desired NAV value in order to silence interfering WiFi nodes in the adjacent channels.

Packet Injection was the most critical of the requirements driving the hardware selection. In all wireless cards, the crucial MAC control functionality like control packet generation (i.e., RTS, CTS, ACK), is implemented in the firmware. Functionality like adding correct headers and flags to DATA packets, adaptive modulation scheme selection, and channel scanning is implemented by the driver on the host device. In the event of a data packet being transmitted, depending on the RTS-Threshold, a RTS packet is generated by the firmware in the wireless card. The driver has little control over the format and contents of the RTS packet.

In the data flow of packet in the wireless card, each packet being transmitted is prepended by the PHY header and the Frame Check Sequence (FCS) field in MAC header is filled in by the firmware. This makes it difficult to generate a raw packet with CTS frame structure from the driver (which runs on the host device) and inject it into the network. Most wireless card firmwares would append a DATA packet header to the bytes being sent by the driver because the driver is not allowed to send control packets.

Atheros Chipset on Madwifi driver [10] provided with a capability to inject packets while in monitor mode. But, to overcome the limitation of wrong headers being attached to the packets by firmware, RAW packet generation library Lorcon2 [4] was used. Lorcon2 creates a virtual interface using the wireless card, making two active virtual interfaces for the card. One virtual interface in monitor mode can passively capture packets on the network, the other virtual interface in transmit mode can send custom frames. A CTS packet is created and transmitted on the air using Lorcon2.

In our experiments, we observed that for each CTS transmission being triggered on Lorcon2, there were 11 copies of the packet being transmitted on air. A wireless packet trace using Wireshark [15], confirmed that the first transmission is the original packet. All subsequent transmissions are re-transmission attempts by the hardware. This was as a result of a bug in the Madwifi driver. While transmitting any packet in monitor mode, the wireless card was waiting for a MAC layer ACK packet. In the absence of the ACK, the wireless card attempted a re-transmission of the packet. The default retransmission limit in Madwifi driver is 10, hence explaining the 11 packets for each transmission. A change in the Madwifi driver to treat monitor mode separately and allow zero retries while transmitting in monitor mode fixed the problem of multiple CTS packets.

TABLE II
WIRELESS CARD DETAILS

Hardware	Details
Wireless Card	TP-Link TL-WN350GD PCI card
Wireless Chipset Chipset	Atheros AR2417
IEEE Standards	54Mbps, IEEE 802.11 b/g capable
Frequency Range	2.4 GHz
Antenna Connector	RP-SMA
Maximum Output Power	18dBm
External Antenna	2 dBi

We use a TP-Link TL-WN350GD PCI wireless card for the experiments. The detailed specifications for the hardware used for the test-bed are summarized in Table II.

As shown in Figure 7, wireless cards in Nodes 2 and 3 are setup in STA mode and are configured to connect to the Access Point. Drivers on Node 2 and 3 are unmodified and use the vanilla versions of driver to operate in normal STA mode. Node 1 is used as a coordinator interface and is setup in monitor mode with lorcon2 to inject customized CTS packets to silence the interfering nodes.

B. Initial Results for WiMAX Protection using CTS Packets by Coordinator Interface

Initially, we determine the effectiveness of the CTS packets with custom NAV duration field. As shown in Figure 7, we start a FTP session from Node 2 to AP and Node 3 to AP. The traffic is generated using Iperf [8] traffic generator. We configure the client nodes in IEEE 802.11g mode, set the Access Point to operate in Channel 1 (center frequency 2.412 GHz) and generate a traffic load of 5 Mbps and 15 Mbps from Node 2 and Node 3 respectively. The FTP flows remain active for a 60 s duration. The CTS packets are injected by Node 1 at 1 ms intervals with NAV of 5 ms. The CTS packet generation starts at 20 s and ends at 40 s. The FTP flows from Node 2 and Node 3 are affected by the CTS packets during the time interval 20-40 s. The observed throughput for both FTP flows by Node 2 and Node 3 can be seen in Figure 8.

From Figure 8, it can be seen that CTS packets transmitted with a constant power can cause the entire WiFi cell in the vicinity of the coordinator interface to remain silent during CTS NAV periods. Since we are flooding the CTS packets at very high rate (1 ms intervals), and the silent period requested in the NAV is 5 ms, there is no scope for any traffic to pass through in the interval of 20s-40 s.

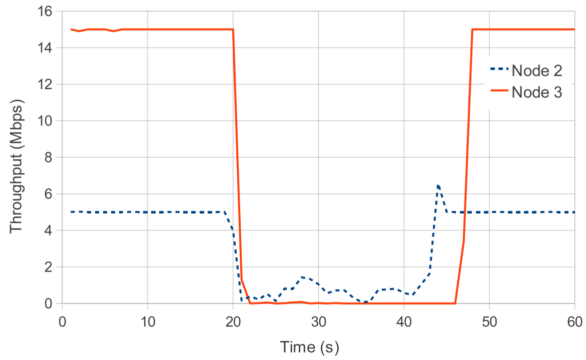

Fig. 8. Impact of CTS Packets Transmitted by the Coordinator Interface on FTP traffic (CTS parameters: Interval=1 ms, NAV=5 ms, Power=5 dBm)

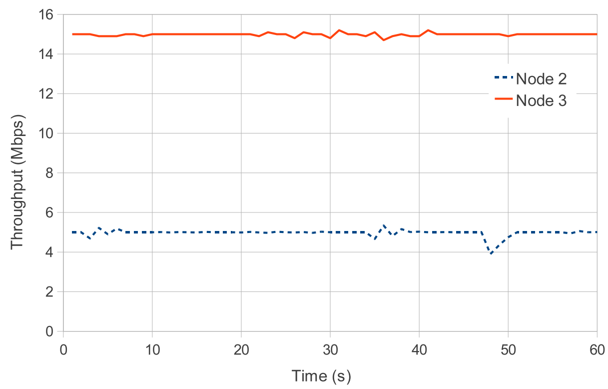

Fig. 9. Impact of CTS Packets Transmitted by the Coordinator Interface on FTP traffic (CTS parameters: Interval=10ms, NAV=5ms, Power=5dBm)

In the next experiment, we increase the interval to 10 ms. This allows for 5 ms silent period every 10 ms. The results are shown in Figure 9. It can be seen that there is very less impact on the throughput of the FTP sessions even with very high rate of CTS packets. With CTS packets every 10 ms and requesting a silent period of 5 ms each, approximately 50% of the air time is reserved in silent periods. As seen in [11] and the references therein, the effective usable throughput from a IEEE 802.11 wireless network is less than 60% of the PHY data rate due to protocol overheads. These protocol related overheads result in idle time being spent by nodes either in Back-off or in protocol mandated silent periods like DIFS and SIFS. Since the total load on the system is 20 Mbps (15 Mbps + 5 Mbps), there is enough spare time to accommodate the requested silent periods without affecting the throughput of data flows.

Discussion: It can be seen from Figures 8 and 9, that no power control on the CTS transmissions by coordinator interface leads to situations where entire adjacent cell is silenced during CTS NAV periods. This is undesirable as the intent is only to block the interfering node in the vicinity of coordinator interface to remain silent.

It is observed that:

1) CTS packets, transmitted by the coordinator interface,

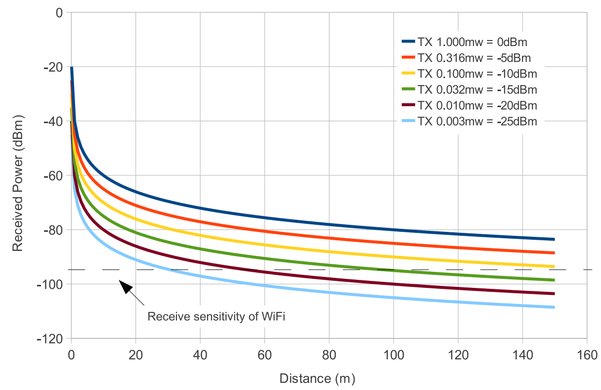

Fig. 10. Free Space Path-loss with Varying transmit power

are effective in creating silent zones without any modification in the STA drivers.

2) CTS packets intervals can be very small and still not affect the throughput of the adjacent wireless network.

The former observation is just an assertion that the CTS scheme works. The latter observation is more important, because the CTS transmissions by the coordinator interface can be used in moderation to protect WiMAX frames without affecting the WiFi network throughput significantly.

VII. Transmit Power Control by Coordinator Interface in the Protection for WiMAX Reception

The results in Section VI-B, show that if the CTS packets from Coordinator interface are triggered very frequently, then it could lead to the entire adjacent WiFi network to suffer. We extend the scheme proposed in Section V-A to enable adaptive transmit power control of the CTS packets. This allows us to limit the extent of silence zone requested by the CTS packets and hence improving the system throughput of the adjacent WiFi network. The path-loss in dB can be computed as,

$$\text{pathloss} = 10log_{10}\left[\left(\frac{4\pi d}{\lambda}\right)^2\right], \qquad (1)$$

Where λ is the wavelength of the signal being transmitted. In our case, for a 2.4 GHz WiFi signal, the wavelength is

$$\lambda = \frac{3.8 \cdot 10^8}{2400 \cdot 10^6} = 0.125\ m.$$

From (1), the received power can be computed as, $P_{received} = P_{transmit} - pathloss$. Figure 10 shows the path-loss for different transmit powers in multiples of 5 dBm steps from a transmit power of 1 mW or 0 dBm. The figure also indicates the noise floor for WiFi devices. The receive sensitivity of WiFi is approximately -96 dBm, i.e. any signal with receive signal strength indicator (RSSI) greater than -96 dBm can be decoded by the WiFi chipsets. Hence, WiFi devices that are located as far as 100 m from the coordinator interface will be able to receive the CTS packets. As a result, all the nodes that receive the CTS packet are forced to remain silent for the WiMAX packet reception at the dual radio

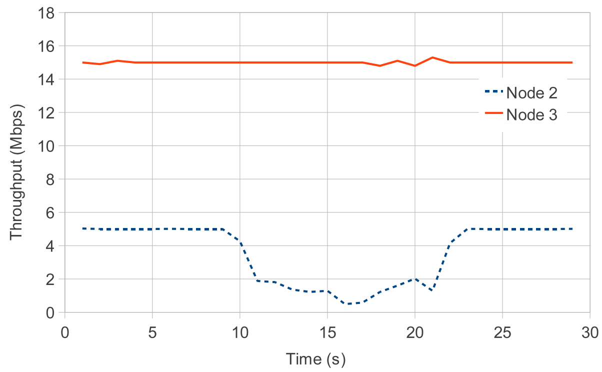

Fig. 11. Impact of CTS Packets Transmitted by the Coordinator Interface on FTP traffic (CTS parameters: Interval=1 ms, NAV=5 ms, Power=-20 dBm)

TABLE III
THROUGHPUT ACHIEVED WITH CTS TRANSMIT POWER = $-20\ dBm$

CTS Interval	1 ms	10 ms	20 ms	100 ms
Node 2	1.34 Mbps	5.002 Mbps	5 Mbps	5 Mbps
Node 3	15 Mbps	15 Mbps	15 Mbps	15 Mbps

node, which is undesirable. Given that the typical range of a commercial WiFi AP is 100 m, we need to transmit the CTS packets at lower transmit powers to limit the silence zone.

As discussed in Section III, the interference from adjacent channel is significant only for a physical separation of 7 m between interfering devices. CTS packets that are received beyond 7 m will not help the WiMAX reception in any way. So, these CTS packets will only decrease the system throughput of the adjacent WiFi network. Theoretically, it can be seen that we need to transmit CTS packets at powers below -20 dBm to control the impact of silence zone created.

A. *Impact of Variable CTS Power Control*

The current wireless drivers do not allow packet transmissions at powers below 1 mW (0 dBm). Hence, for the purpose of this study, we attach RF attenuators to the coordinator interface to reduce the transmit power below 1 mW.

Figure 11 shows the results for transmission of CTS with power -20 dBm and interval of 1 ms. Comparing the results with Figure 8, where no power control is used, the FTP flow for Node 3 is unaffected by the CTS packets. Node 3 is located at a distance of approximately 17 m separated by a few wooden partitions. This allows enough margin for Node 3 to ignore the CTS packets and continue its transmissions. It should be noted that the CTS packets are injected in the network at a very high rate (interval of 1 ms and NAV of 5 ms), and in actual practice the interval will be higher. This will result in better throughput for Node 2 in normal circumstances. This also ensures that only the nodes that are in the vicinity of the coordinator interface and hear the CTS packets remain silent for the duration of CTS transmissions. Table III, shows a summary of throughput achieved for various CTS intervals. It can be seen that the throughput of Node 2 is affected only under high stress conditions of CTS intervals. The results in Table III are for the duration between 10 s and 20 s as seen in Figure 11 when CTS packets are being transmitted.

We illustrate the performance impact on WiFi throughput due to the CTS packets with an example. Consider a WiMAX SS with a downlink load of less than 2 Mbps, and a WiMAX system throughput of at least 12 Mbps (minimum SINR = 12 dB, minimum modulation scheme 16QAM-3/4). In the best case scenario, downlink subframes optimally packed by the BS in as few frames as possible, the SS needs one out of every six frames to be protected. In this case, the CLC Controller will generate a CTS packet every 30 ms (one frame = 5 ms). In an average case, when the downlink subframes for the WiMAX SS are not optimally packed, the CLC Controller may need alternate WiMAX frame to be protected. The CTS interval in this case would be 10 ms. From the results in Table III, it is clear that the WiFi network performance would not be affected in both the cases.

ACKNOWLEDGMENT

The authors would like to thank Siddharth Shetty for the insightful discussions during the research. The authors would also like to thank the anonymous reviewers for the valuable feedback on improving the paper. This research is partially supported by TTSL-IIT Bombay Center of Excellence in Telecommunications (TICET).

VIII. CONCLUSION AND FUTURE WORK

We have demonstrated how a spare IEEE 802.11 radio interface, on a multi-radio platform (IEEE 802.11 and IEEE 802.16 interfaces), can be used effectively to mitigate adjacent channel interference. We also demonstrate that the CTS-to-Self packets generated by the coordinator interface to protect WiMAX transmissions do not affect the performance of the WiFi network operating in the adjacent channels. We also demonstrate, with experimentation, that power control can be used effectively to limit the silence zone created by CTS-to-Self packets triggered by the WiMAX transmissions. We have also proposed schemes to protect WiFi transmissions by invoking CLC messages to the IEEE 802.16 BS to modify its schedule according to the WiFi activity.

As a part of the future work, we intend to perform experimental trials on WiMAX networks by sending CLC messages to the IEEE 802.16 BS to protect WiFi frames. We also intend to study methods to extend this scheme to other 4G technologies like LTE-Advanced.

REFERENCES

[1] "Recommendations On Allocation and Pricing for 2.3-2.4 GHz, 2.5-2.69 GHz & 3.3-3.6 GHz bands," http://www.trai.gov.in/WriteReadData/Recommendation/Documents/recommendation11july08.pdf.

[2] "IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Broadband Wireless Access Systems," *IEEE Std 802.16-2009*, 2009.

[3] "IEEE Standard for Information technology — Telecommunications and information exchange between systems Local and metropolitan area networks — Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2012*, 2012.

[4] 802.11 Ninja, "Loss Of Radio CONnectivity (LORCON2)," http://802.11ninja.net/.

[5] R. Aiello and S. Shetty, "Testing Raises Concerns over 802.11-based High-speed Bluetooth," *EE Times*, March 2008, http://eetimes.com/design/automotive-design/4012958.

[6] C. F. Chiasserini and R. R. Rao, "Coexistence Mechanisms for Interference Mitigation between IEEE 802.11 WLANs and Bluetooth," in *IEEE Infocom*, vol. 2, 2002, pp. 590 – 598.

[7] "InSSIDer, WiFi Network Scanner by *MetaGeek*," http://www.metageek.net/products/inssider.

[8] iperf, "Internet Protocol Traffic Generator," http://iperf.sourceforge.net/.

[9] J. Kim, S. Park, S. Rhee, Y.-H. Choi, and H. Hwang, "Energy Efficient Coexistence of WiFi and WiMAX Systems Sharing Frequency Band," in *Future Generation Information Technology*, ser. LNCS, vol. 6485, 2010, pp. 164–170.

[10] Madwifi, "Madwifi Project," http://www.madwifi-project.org.

[11] P. Rathod, O. Dabeer, A. Karandikar, and A. Sahoo, "Characterizing the Exit Process of a Non-Saturated IEEE 802.11 Wireless Network," in *Proc. of ACM Mobile Ad Hoc Networking and Computing (MobiHoc '09)*, 2009, pp. 249–258.

[12] M. M. Siddique, B.-L. Wenning, C. Gorg, and M. Muehleisen, "Spectrum Sharing between IEEE 802.16 and IEEE 802.11 based Wireless Networks," in *IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM)*, June 2010, pp. 1 –6.

[13] N. J. Thomas, M. J. Willis, and K. H. Craig, "Analysis of Co-existence between IEEE 802.11 and IEEE 802.16 Systems," in *Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on*, vol. 2, Sept. 2006, pp. 615 –620.

[14] E. G. Villegas, E. Lopez-Aguilera, R. Vidal, and J. Paradells, "Effect of Adjacent-Channel Interference in IEEE 802.11 WLANs," in *Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, August 2007, pp. 118 –125.

[15] Wireshark, "Network Protocol Analyzer," http://www.wireshark.org/.

[16] X. Yang, X. Yang, J. Zhu, and H.-Y. Liu, "Collocated Radio Coexistence Method," USA Patent US 7 907 572B2, 03 15, 2011, http://www.patentlens.net/patentlens/patent/US_7907572B2/.

[17] S. Zhan, A. Waltho, X. Guo, C. Chen, and A. Bettner, "Performance Analysis and Design Considerations for Multi-Radio Platforms," *Intel Developer Forum Report*, 2006.

[18] J. Zhu and H. Yin, "Enabling Collocated Coexistence in IEEE 802.16 Networks via Perceived Concurrency," *IEEE Communications Magazine*, vol. 47, no. 6, pp. 108–114, June 2009.