Microwave Oven Interference with 802.11

Mayank Kabra and Joseph Sarlo

CSE 222A
23 March 2006

1. Introduction

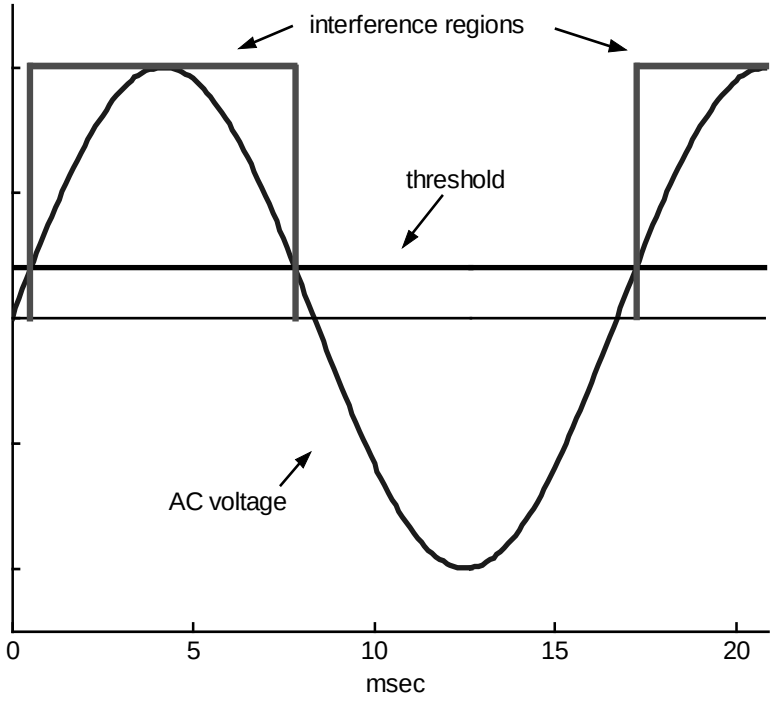
Microwave ovens and 802.11 both use the unlicensed 2.4GHz ISM (Industrial Scientific Medical) band. Microwave ovens use this frequency to heat while 802.11 uses this for communication. The use of microwave ovens in the vicinity of an 802.11 node therefore naturally affects the node's ability to communicate. In this project we investigate how microwave oven noise interacts with 802.11 communication protocol.

2. Microwave Ovens

As the waves in microwave are used to heat food, the generated waves are very powerful. Even though shielding is provided to make sure that waves do not escape the microwave enclosure, some of it does escape. In comparison to the 802.11 signals, which have power in the milliwatts range, the waves that escape from the microwave are very powerful.

The main component of a microwave oven is a magnetron. The magnetron generates high power electromagnetic waves whenever its input voltage is above some threshold. A.C. mains normally drive the magnetron. The A.C. mains can also be rectified before being supplied to the magnetron. In either case, when the input voltage is less than the threshold, no magnetic waves are generated. Whenever the A.C. mains voltage is below some threshold, no waves would be generated. So whenever a microwave oven is being used, it does not generate waves throughout the time it is switched on. As the A.C. mains are periodic with a frequency of 60Hz, the time intervals when no waves are generated by magnetron are also periodic with the same frequency.

The value of threshold and the use of a rectifier is manufacture dependent and hence varies from microwave to microwave.



3. 802.11

Not all 802.11 protocols use the 2.4GHz band. Only 802.11b and 802.11g communicate using the 2.4GHz band. As the strength of 802.11 signals is much weaker than interference generated by microwave oven, a signal transmitted while there is interference will not be received properly. In other words, microwave oven interference drowns out any other signal that may be present.

Contention for media is avoided in 802.11 by doing carrier sense. 802.11 hardware uses RF transceiver to transmit and receive signals. These are used to check if some signal is being transmitted. This process is called carrier sensing. If some signal is present, then the medium is assumed to be busy. Whenever a medium is busy no transmissions are made.

802.11 defines following rules for transmissions:

- If the medium has been idle for longer than a specific amount of time called DIFS (DCF inter-frame space), transmissions can begin immediately.
- If the medium is busy, the node must wait for the channel to become idle. 802.11 refers to the wait as access deferral. If access is deferred, the station waits for the medium to become idle for the DIFS. A period called the contention window or back-off window follows the DIFS. This window is divided into slots. Nodes pick a random slot and wait for that

slot before attempting to access the medium. All slots are equally likely to be selected. When several nodes are attempting to transmit, the node that picks the first slot wins. The back-off time is selected from a larger range each time a transmission fails.

4. Microwave and 802.11

Whenever the microwave is generating interference, it is not possible to transmit any signal. The only time 802.11 can send frames is when there is no interference. For example, if the microwave oven interference is present for 60% of the time, 802.11 can transmit only 40% of time. This implies that the average bandwidth of 802.11 cannot be increased beyond 40% of the original.

Suppose the microwave interference starts when no packet is being transmitted. In this case, all the nodes see the medium as busy and do nothing. So the state of the system when the interference is gone is the same as the state when the interference started. This implies that the microwave interference does not interact with 802.11 except for making the medium unavailable.

If a frame is being transmitted when the microwave interference begins, the receiver will not decode the frame properly. In this case, the transmitter will increase its back-off period for the next transmission. This may lead to reduction of bandwidth as seen by the system. For example, consider two cases: one where the frame is transmitted successfully and then the interference starts and another where the frame is not transmitted successfully. When the next frame needs to be transmitted the node will much smaller time when the transmission is successful. Due to this the waiting time increases and the free medium is not used as often as it could have been used. Also the retransmission of corrupted frame will decrease the perceived bandwidth.

Decreasing the probability of its occurrence can reduce the loss of bandwidth due to frame corruption. Making frame size smaller and not decreasing the transmission speed can achieve this. Reduction in frame size reduces the transit time of the frame. In case of frame losses 802.11 nodes may try to reduce the transmission speed. But in case of microwave interference this will increase the transit time, which will in turn increase the probability of corruption of frames. So when microwave oven interference is present, the transmission speed should not be decreased. Both of these schemes are already implemented in commercial 802.11 products [2].

Also, 802.11 supports fragmentation of data, which can be used to counter such losses. A packet to be transmitted is broken up into smaller fragments. After transmitting each fragment, the sender waits for the receiver to acknowledge. So if the interference starts when some packet is being transmitted, only one fragment of the packet will be lost and not the whole packet.

We tested the bandwidth performance of 802.11 in presence of microwave oven interference for both TCP as well as UDP. The microwave oven that was used generated

interference for almost half the time. TCP bandwidth decreased from around 11Mbps to 5Mbps when the microwave was switched on. This is as expected. For UDP the performance degraded from 30Mpbs to 15Mpbs. This again aligns well with our expectation that the bandwidth will degrade to half. These experiments also confirm the fact that 802.11 makes full use of available time to give the maximum possible bandwidth.

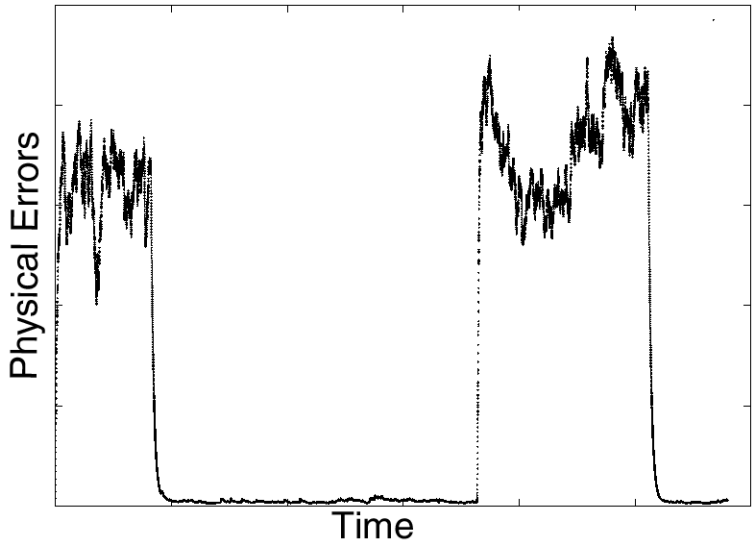
5. Implementation

From above we can see that it is not possible to improve the performance of 802.11 in the presence of microwave oven. But there may some applications that may benefit if we could detect when a microwave is on and predict when the microwave interference is going to be present while the microwave is active. These techniques were implemented in Linux by modifying MADWiFi drivers for Atheros-Netgear WAG511 PCMCIA NIC [5].

6. Detecting Interference

The way in which microwave oven interference interacts with 802.11 hardware makes it possible to detect the presence of the interference. The interference is interpreted by the hardware as a signal transmission. However, errors are encountered when an attempt is made to decode this interference signal. The hardware reports this event as a physical error. Because of this, the number of physical errors reported by 802.11 hardware increases significantly when microwave oven interference is present.

The figure below was extracted from a trace of the *Jigsaw* [1] dataset and shows the number of physical errors encountered during a period of approximately 10 minutes. The two regions in which the number of physical errors are significantly high correspond to periods of time when microwave oven interference was encountered and can be clearly discerned from the nominal levels where no interference was present.



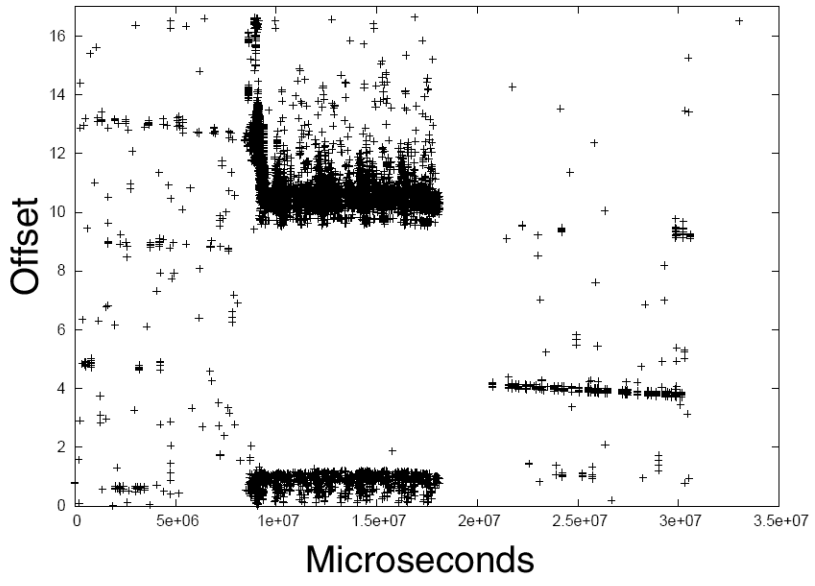
We can make use of this behavior to detect the presence of microwave oven interference. Specifically, we average the number of physical error occurrences reported by the hardware over time and compare this average to some threshold value to detect whether interference is present. Our experiments suggest that an exponentially weighted time-averaging technique is most successful in eliminated false positives. We also found that an averaging period of 250 to 500 milliseconds is sufficient for most situations. We have further seen that while the number of physical error occurrences varies both from oven to oven and as a function of the distance from the interference source, the number of physical error occurrences commonly increases 3 to 10 times above the nominal level in the presence of microwave oven interference, and the threshold can be set accordingly.

7. Interference Synchronization and Prediction

Due to the periodic nature of microwave oven interference, it is possible to predict the windows in time for which the interference will and will not be present while the microwave oven is active. To accomplish this, we synchronize the physical error occurrences with the frequency of the interference signal, specifically 60 Hz. We employ an *offset* as described below:

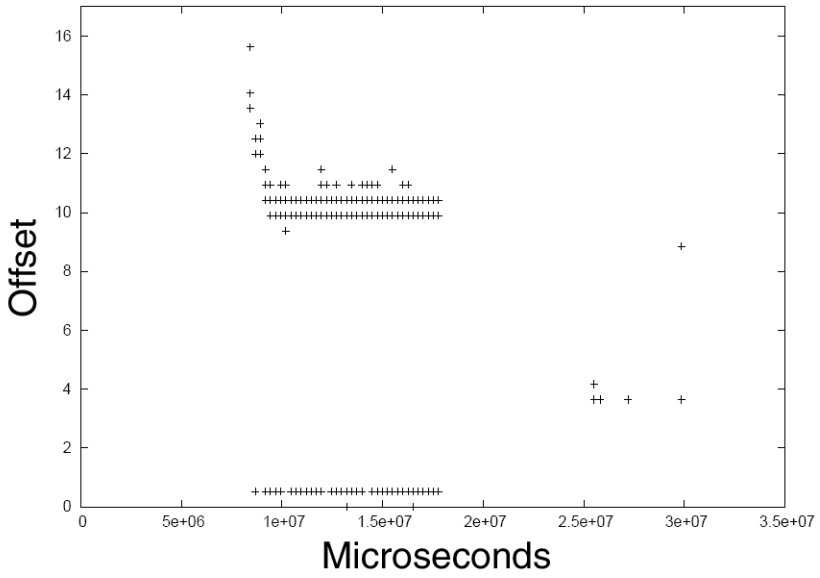
$$offset = time - \left\lfloor \frac{time}{T} \right\rfloor * T;\ T = \frac{1}{60}$$

where *time* is the time at which a physical error has occurred. This *offset* can be considered as the time when the physical error occurred modulo a 1/60 second period. Perhaps a more intuitive and useful interpretation is that it gives the phase of the physical error occurrence within the 60 Hz cycle. Since the microwave oven interference is periodic at 60 Hz, the *offset* values for the physical error times will remain constant while the microwave is active.



The figure above shows the *offset* values for a period of approximately 35 seconds in which a microwave oven was activated after approximately 1 second and for a period of approximately 8 seconds. Each graph mark indicates a single physical error occurrence. The two dense regions correspond to the physical errors caused by the microwave oven interference. The flatness of these regions demonstrates the periodicity of the interference. Furthermore, since there are two distinct regions, it can be deduced that an AC rectifier was used to generate the microwaves causing the interference. We note another periodic occurrence that can be seen as a thin line beginning at approximately 22 seconds. This region does not correspond to the interference from the previously mentioned microwave and must be the result of some other interference source.

Since the microwave oven interference is periodic, we can not only detect the interference, but also predict when the physical errors will occur by using the synchronization *offset* values of previous physical errors. To accomplish this, we classify the *offset* values of the physical error occurrences into 32 clusters by dividing the period of the 60 Hz cycle into 32 sub-windows and counting the occurrences of physical errors for each sub-window. We then periodically compare these counts to some threshold value to determine when the interference occurs with respect to the period. We can then simply predict that the *offset* values will remain constant for the periods in between the threshold comparisons.



The figure above shows the results of this prediction technique for the instance described above. We can see that the two regions corresponding to the microwave interference are properly predicted and that the region of the unknown interference source is partially predicted as well. Furthermore, we see only one false positive occurring for this sample.

8. Acknowledgement

We would like to thank Yu-Chung Cheng for providing us with *Jigsaw* 802.11 traces and the wireless card.

9. Conclusion

In this project we characterized the microwave oven interference and investigated how the interference interacts with 802.11. We found that it is not possible to improve the performance of 802.11 significantly in the presence of microwave oven interference, as the performance of 802.11 is already nearly optimal. We implemented a microwave oven interference detector and predictor, which is able to provide the information with high accuracy.

10. References

1) Yu-Chung Cheng, John Bellardo, Peter Benko, Alex Snoeren, Geoff Voelker and Stefan Savage, "*Jigsaw: Solving the Puzzle of Enterprise 802.11 Analysis"*, UCSD Tech Report, CS2006-0849, Feb 2006.

2) "*Microwave oven robustness*", ORiNOCO Technical Bulletin 035/A, Feb 2000.

3) Matthew S. Gast, "*802.11 Wireless Networks*", O'Reilly and Associates, April 2002.

4) " *Information technology – Telecommunications and information exchange between systems- Local and metropolitan are networks – Specific requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"*, IEEE Standards 2003.

5) MADWiFi Atheros driver for Linux, 2003, http://sourceforge.net/projects/madwifi/