People Counting using USRP and IEEE 802.11b

Nasidul Islam
College of Engineering and Computing
Florida International University
Miami, Florida 33174
Email: nisla004@fiu.edu

***Abstract*—The objective of this project is to use NI USRP to count the number of people in a general area. It is done by successfully designing a logic in LabView to detect and decode probe requests and determining the MAC address of all possible wireless enabled devices. The number of unique MAC addresses found can be safely assumed to be the number of people in that area. This idea has been explored and implemented to a limited success in this project.**

I. Introduction

NI USRPs are software defined radios (SDRs). SDRs are special equipments that function just like regular radios, but instead of having the mixers and filters implemented in hardware, they are implemented in software. This makes for a very versatile range of operations for the equipment since all the features can be very specifically tuned.

Fig. 1: NI USRP 2930

These devices are interfaced with a computer using software called LabView. The SDRs will then be properly configured using Virtual Instruments (VIs) to perform specific operations, which will be able to pick up the probe requests of WiFi devices. WiFi devices have a lot of standards to follow; for this project, the IEEE 802.11b standard protocol was followed. Whenever a device turns on its WiFi capabilities, it periodically sends out probe requests in an attempt to find all available WiFi networks and/or connect to an existing one from memory. These probe requests contain the MAC addresses of the device, and every device has a unique MAC address. Therefore, the number of unique MAC addresses decoded in an area can be assumed to be the number of people in that area.

II. Methodology

The entire IEEE 802.11 is the WiFi standard. There have been several amendments made to it and not all parts of the standards (such as a/b/g/netc) follow the same protocol. For this project, the 802.11b was followed, which employs DSSS, instead of OFDM, for modulation. However, regardless of what modulation technique is used, they all use the same frame structure for the management frame. A certain number of first bits is the MAC header, while the rest is the frame body. This is illustrated below

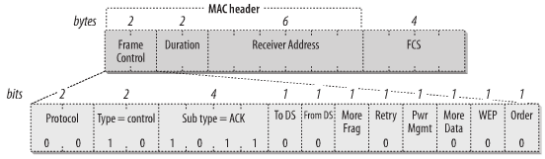

Fig. 2: ACK Frame Format

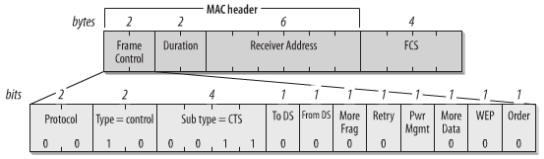

Fig. 3: ACK Frame Format

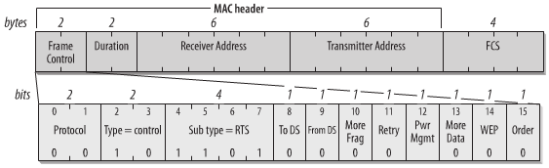

Fig. 4: RTS Frame Format

Therefore, it was a matter of the start and end index value through which the frame structure needs to be checked to find the MAC address. In order to do this, an ad-hoc network was setup. The network was named '$WiFi_Test$' successfully set up and live and waiting for users to connect to it. The data packets sent over this network and their respective power was recorded. The trigger threshold was increased from the default value to differentiate the actual data packets from noise and other unwanted elements in the wireless channel. This was implemented in LabView, and the following front panel view was obtained

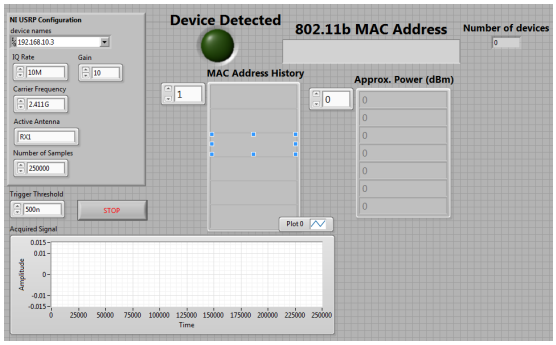

Fig. 5: Front Panel of LabView Interface

This logic was successful at serving its purpose. It was able to detect and decode the MAC addresses to a certain degree of precision. The VIs were also designed to capture the received power. This can be used to determine the distance of the user from the USRP using basic path loss models.

However, when trying to decode the SSID of the $FIUWiFi$, some problems came up. The $FIUWiFi$ (for visitors only) showed similar results to the one shown above, but the $FIU_SECUREWiFi$ was proving more of a challenge. It was configured to hop frequencies, and since the VI only allows to scan a certain frequency at a time, the exact frequency at which the network was transmitting at the moment was difficult to determine. The figure below shows the frequency overlapping of the 2.4GHz frequency used by WiFi

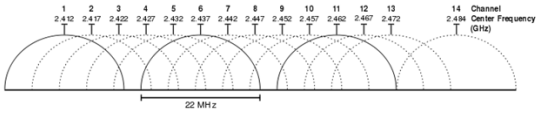

Fig. 6: Graphical representation of 2.4 GHz band channels overlapping

There were some problems faced while conducting this project.

- The noise would jumble up certain bits of the obtained MAC address. As a result, some parts would be correct while the other parts were distorted by noise. This was mitigated by scanning through different channels and increasing the trigger threshold
- The noise would sometimes also make totally incorrect, ghost MAC addresses appear on the front panel, even if there were no WiFi devices nearby. This was not entirely mitigated, however an idea was thought of to do so. That is to construct a lookup table. Since this would be implemented in an area where there is mostly a known population. Therefore, when a MAC address appears, it will be first checked against a lookup table, it will be counted as a legit device. If not, then it will be ignored as garbage value.
- When deployed in a very crowded scenario (the EPA P3 Expo), it was seen to perform to a very limited capacity. A lot of radio interference from various different equipments in the environment seriously deteriorated the USRPs ability to detect the probe requests. This problem could not be taken cared of, and this could be a line of research in the future. However, the VIs worked quite well if the user was very close to the USRP.

III. Conclusion

The idea of counting the number of people in an area using USRPs is very interesting. With the proper logic, this can very accurately serve its purpose. This idea can also be used to triangulate the exact location of the user using the receiver power and basic path loss models. However, it also has its limitations. The technology has failed to perform to a satisfactory extent in a large, extremely crowded situation with lots of radio interference. The logic can be improved to nullify the effects of noise on the received values of the MAC addresses.

References

[1] [1] Matthew Ghast, ”802.11 Wireless Networks: The Definitive Guide”, O’Reilly Media, Inc. April 23, 2002
[2] $http://en.wikipedia.org/wiki/List_of_WLAN_channels$