Wi-Fi Traffic Analysis

Prasidh Srikanth
Department of Computer Science
Stony Brook University
StonyBrook, NewYork, USA
631-466-4922
psrikanth@cs.stonybrook.edu

Chidambaram Ramanathan
Department of Computer Science
Stony Brook University
StonyBrook, NewYork, USA
631-706-5034
cramanathan@cs.stonybrook.edu

ABSTRACT

Wi-Fi is a popular technology that allows devices to exchange data without any physical connection [7]. It is widely made use of these days and present almost everywhere. One of the main reasons of their popularity is because of the ease of their installation and wide coverage. Though Wi-Fi is widely used, there has been less interest in exploring the performance and usage patterns. A clear understanding of the above can be obtained by collecting traces and making an intuitive analysis on the data captured.

The aim of our project is to analyze the Wi-Fi traffic in various busy spots on the Stony Brook University's campus and come up with interesting findings. Our work revolves around collecting traces using a network sniffer such as Wire Shark and analyzing the captured packets. We study the traces to find patterns and try to establish a relationship that best describes the status of the 802.11 Wi-Fi network. We have considered to analyze the networks WolfieNet-Secure, WolfieNet-Guest, WolfieNet-Open, WolfieNet-Get-Connected which are widely available throughout the campus. We have chosen certain busy places such as the Health Sciences Library, Melville Library, Computer Science Lobby and University Hospital. With the available traces, we make intuitive analysis and draw graphs to substantiate our claims.

General Terms

Measurement, Documentation, Experimentation, Theory, Performance.

Keywords

Wireless Traffic, Packet capture analysis, 802.11 performance

1. INTRODUCTION

Wireless LANs are most prevalent in Stony Brook University and mobile users are on the rise throughout the university campus. Stony Brook University is a public research university with a sprawling campus spread across 1,364 acres. There are about 24,500 students enrolled in the main campus and they have access to Wi-Fi communication throughout the campus [1]. The WolfieNet (Stony brook University's Wi-Fi network) is available to all students, faculty, staff and guests. Wi-Fi hotspots are abundant at all busy places and we focus our Wi-Fi traffic research to analyze the coverage in Students Activities Centre, Computer Science building, Frank Melville Jr. Memorial Library, Health Science Center library and campus residence houses(Chapin Apartments).

With growing number of devices seeking to connect to the network, our research interest is pertaining to the quality of service (performance and throughput), signal strength, packet loss and transmission rate of the Wi-Fi users on campus. There are 4 categories of WolfieNet network and they are as follows:

WolfieNet-Get-Connected mainly for use by people trying to connect to the network for the first time.
WolfieNet-Secure for all students, faculty and staff.

WolfieNet-Open available at residence halls and to be used by people using gaming systems.

WolfieNet-Guest for use by the visitors of the university [2].

2. PACKET CAPTURE

In this section, we discuss how we have captured the packets. We have captured the 802.11 packets by making use of wire shark and the commands we make use of to filter packets such as RTS/CTS, ACKs, etc are as follows:

1. Association requests: These are the signals sent by a mobile station to a BSS (Basic Service Set) requesting connection.
   Filter: wlan.fc.type_subtype==0x00

2. Association response: These are the response sent by a BSS to a mobile station that requested connection.
   Filter: wlan.fc.type_subtype==0x01

3. Reassociation requests: These are the signals sent by a mobile station changing association to another AP in the same ESS (Extended Service Set).
   Filter: wlan.fc.type_subtype==0x02

4. Reassociation response: These are responses to the Reassociation requests.
   Filter: wlan.fc.type_subtype==0x03

5. Beacon: These are signals sent by an APP providing information about the BSS.
   Filter: wlan.fc.type_subtype==0x08

6. Requests to send frame(RTS):
   Filter: wlan.fc.type_subtype==0x1B

7. Clear to send frame(CTS):
   Filter: wlan.fc.type_subtype==0x1C

8. Data frame: This is the frame containing data.
   Filter: wlan.fc.type_subtype==0x20

3. RESULTS

In the following section, we analyze the performance of the IEEE 802.11 network on campus through various graphs.

A. Cross section of the IEEE 802.11 network

We studied the broad category of packets prevailing in the IEEE 802.11 network by analyzing the various packets captured. The packets can be put under three main categories. (I) *Management frames* (II) *Control frames* (III) *Data frames.* Control frames are the backbone of a Wi-Fi network. It employs several mechanisms in order to successfully capture a packet through the air. The following diagram (Figure 1) shows a cross section of the network during one such instance of the capture.

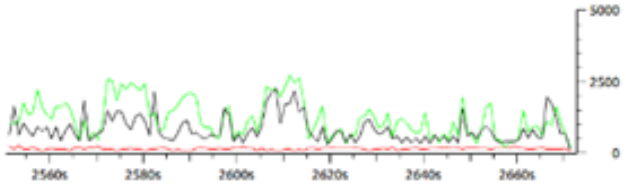

Figure 1: Control frames, data frames and management frames

The green lines correspond to the Control frames, the black line corresponds to the Data frames and the red line corresponds to the Management frames. The Control frames include RTS, CTS, ACK and other packets. The Management frames include ASSOCIATION REQUEST, ASSOCIATION RESPONSE, REASSOCIATION REQUEST and RESPONSE. PROBE REQUEST and RESPONSE and other packets. The data frames are those sent by the users.

B. Throughput in an IEEE 802.11 network

We now study, how effectively the network is actually used to send data. In other words, we try to measure how far the network serves the users keeping aside the internal overhead of the management of the network. The following chart (Figure 2) compares the bandwidth used to send data packets and the management/control packets.

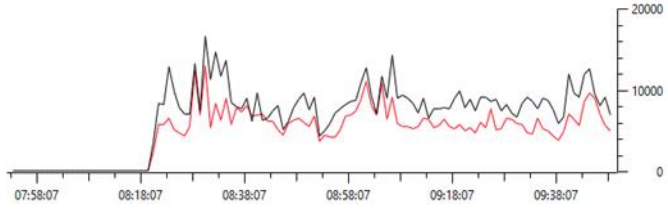

Figure 2: Overall packets excluding data packets vs data packets

The black line corresponds to the overall packets transmitted excluding the data packets. The red line is the amount of data packets. We can realize that, the performance of the network is not entirely optimal. The network never attains 100% efficiency. This capture was taken in the Melville library in the collaborative study area where students study together. It can be seen, even for such a small network, many additional packets are sent in order to actually send and receive data packets. If we consider critical scenarios like an Airport or a Market, we anticipate the situation to get worse and the effective throughput to reduce.

C. Retransmission in the network

We also attempt to measure throughput by considering the failure in the transmission of a packet, leading a client to retry sending the packet. The following diagram (Figure 3) illustrates what percentage of the network is wasted due to failure in transmissions.

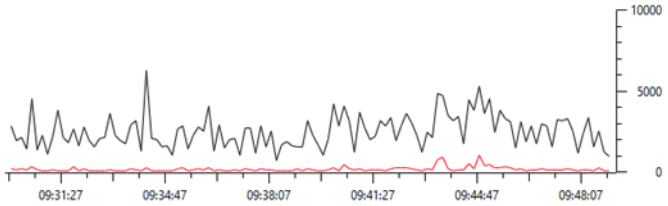

Figure 3: Total packets (black) vs retransmitted packets (red)

We tried this experiment in Melville Library, University Hospital and Computer Science Department. In all the case, the effort spent in retransmitting a packet was minimal. The spots chosen were such that there were obstructions.

D. Roaming in the network

We tried to analyze the network in order to find how many clients are actually mobile. To our surprise very few clients move from AP to the other. This can be used as a great cornerstone in designing an IEEE 802.11 network. We attach the graphs taken at three different places.

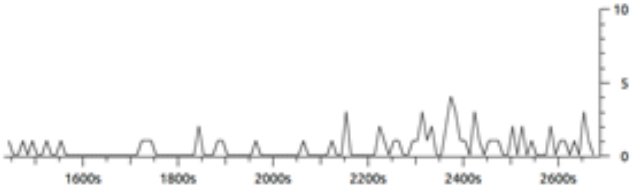

Figure 4: Roaming in HSC library

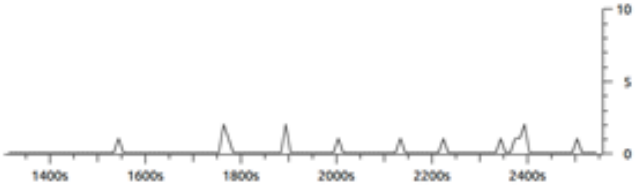

Figure 5: Roaming in Computer Science Department

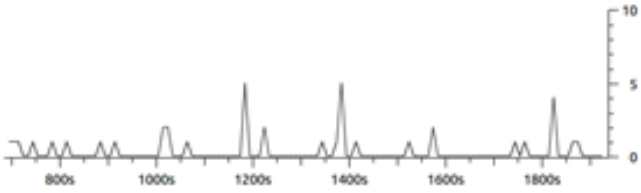

Figure 6: Roaming in Melville library

We can clearly see that the number of clients attempting to roam is substantially lesser when compared to the traffic in the network. This will at least be true in the case of places like Universities, Hotels, Libraries and other places where people are not expected to move much around the place. This property can be exploited so that we can design the AP's in a very efficient manner reducing the complexity in serving the client's

roam request. AP's can also be placed in strategic locations so that, it minimizes the handoffs required in the network.

E. Load in the network

We captured packets from a particular location over an extended period of time in order to find out how much amount of bandwidth is taken away by the protocol. We considered a simple instance of the *Beacon* frames sent by the AP's in order to advertise their presence. The main advantage of this method is that, a client can quickly find out another AP when it loses contact with the AP it has been previously associated with. Though this seems like an obvious advantage we try to find out a hidden tradeoff behind this. Consider the following scenario (Figure 7) taken in the University Hospital

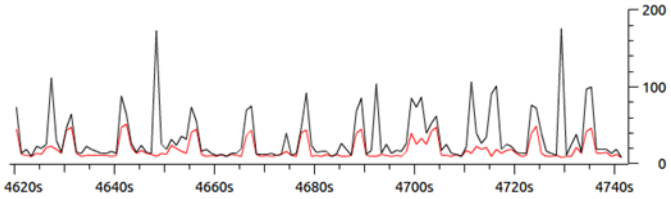

Figure 7: Total packets vs beacon signals

The black line shows the overall packets sent by an AP. The red line shows the total number of *Beacons* sent by the same AP. It can be clearly seen that the beacons occupy almost 50% of an AP traffic. From the wire shark captures, it was deduced that each AP was configured to send a beacon for every 10ms. This might be more suitable in an environment where clients are expected to be mobile. But consider a place like a Library or a Hospital or any other place where most number of clients are expected to be stationary. In this case, sending a beacon every 10ms would be considered not so useful. Instead the AP could take some intuitive measures and manage the rate at which it sends the control frames. This would reduce the congestion in the IEEE 802.11 network and also reduce contention for the medium. This would also be a power saving technique as a lot of power required to generate packets are saved.

F. Load balancing

We tried to survey a place by analyzing the top three SSID's the clients are connected to. SSID is the name of a network. Many AP's can be a part of a SSID. Thus by trying to know to which SSID, most number of clients are connected to, we can alter the design of the network in a particular place. For example, we could do this experiment in each place for about 10 days and try to find a pattern in which the clients connect. By observing this pattern, we can get a wealth of information. Consider the following experiment (Figure 8) which we did in Melville Library for a period of 3 days.

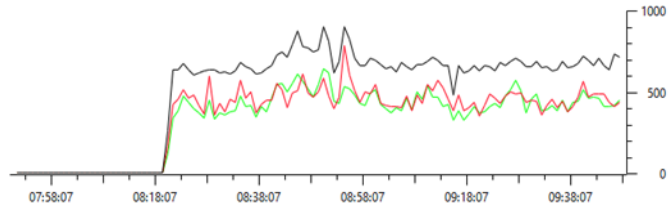

Figure 8: Packets in Melville library

The black line corresponds to WolfieNet-Get-Connected, the red line corresponds to Wolfienet-secure and the green line corresponds to WolfieNet-Guest. We were able to infer that at this time, clients were always getting connected to the WolfieNet-Get-Connected network. Thus we could identify certain hot spots and make an informed decision of placing the AP's. With such a positioning, more clients could get connected to the network and hence we could increase the throughput users get.

F. Statistics of users in a network

Analyzing the 802.11 traffic can have several benefits behind it because it gives us a lot of additional information. It can have various commercial uses as well. By analyzing our 10 day packet capture, we tried to find out what percentage of users use devices like Apple, Intel etc. To our surprise more than 70% of the users present during the live capture were using devices produced by Apple. This information can be tapped to add more features in the Wi-Fi network. This in turn can also increase user happiness.

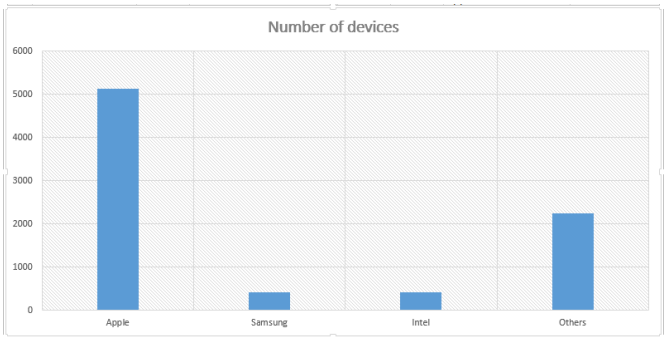

Figure 9: Comparison of devices used by people on campus

From the above graph, it can be seen that most of the users use Apple device. With this information several parameters can be tuned which can result in the creased productivity of the network.

4. RELATED WORK

Our main motivation behind carrying out Wi-Fi traffic analysis was to understand the activity of Wi-Fi traffic in the Stony Brook University's Wolfie-Net. We had similar network analysis carried out extensively in Dartmouth as mentioned in [3]. They had carried out an extensive trace of their wireless network over a span of around 70 days. They were able to gain more insight about the network as they had configured their access points on campus to transmit syslog messages for their events of interest. Our analysis however has been able to provide insights on the peak usage time and places of Wi-Fi traffic on campus, distribution of devices among people on campus and overall performance of the network.

5. CONCLUSION

Wi-Fi traffic snooping that we carried out for ten days on campus helped us gain and provide an insight on the performance of the WolfieNet network. We realized that the network usage was very high in the evenings as most students study starting at that time continuing till early in the morning. Since most of the students prefer to study together, they are more prevalent in the libraries (the ones in Health Science Center and the main library). This led to consumption of most of the network bandwidth at these locations thus creating congestion, packet loss and reduced performance. We found that few cards are connected only for a short period of time and few roam within the sessions. We clearly see that there is high activity in areas where students study together and hence need for better coverage such. We also

found that most users remain stationary within a session even though they use wireless connection.

6. ACKNOWLEDGMENTS

Our sincere thanks to Professor. Samir Das and Mr. Ayon Chakraborty of Stony Brook University for providing us with their insight on packet capture and Wi-Fi traffic analysis.

7. REFERENCES

[1] Wikipedia article on "Stony Brook University" (Last modified on 9, December 2013), http://en.wikipedia.org/wiki/Stony_Brook_University

[2] WolfieNet (Wi-Fi), http://it.stonybrook.edu/services/wi-fi-wolfienet

[3] David Kotz and Kobby Essien (March 12, 2002), "Characterizing Usage of a Campus-wide Wireless Network", http://delivery.acm.org/10.1145/580000/570659/p107-kotz.pdf

[4] Display filter Reference: IEEE 802.11 wireless LAN, http://www.wireshark.org/docs/dfref/w/wlan.html

[5] 802.11 Sniffer Capture Analysis – Wireshark filering (May 28, 2012), https://supportforums.cisco.com/docs/DOC-24730

[6] IEEE 802.11 standard (June, 12 2007), https://www.dropbox.com/s/frtagyvha4avxsw/802.11-2007.pdf

[7] Wikipedia article on "Wi-Fi" (Last modified on 16, December 2013), http://en.wikipedia.org/wiki/Wi-Fi

[8] Organizationally Unique Identifiers OR Company ID, http://standards.ieee.org/develop/regauth/oui/oui.txt