Wireless Impairments Detector

Israel Márquez Salinas
Université Pierre & Marie Curie
s.marquez.israel@gmail.com

ABSTRACT

Home WLANs have become an essential element in households nowadays. The preferred method to access Internet from home is WiFi. Home WLANs have brought their benefits and challenges into the home. The variety and complexity of WiFi and non-WiFi devices make Home WLANs keen to experience WiFi impairments. Identifying these impairments can be challenging, even for Wireless experts. To approach this challenge we have begun to develop a tool to identify WiFi issues in Home WLANs. In this paper we present the initial stages to develop the basis of this tool. We have conducted experiments triggering Wireless and non-wireless issues in a testbed. During these experiment sessions we have collected metrics from different components in the setup. Metrics have been collected using active and passive measurement techniques, a description of these two techniques is covered in section 2.1. Finally we consolidate and correlate these metrics to identify when a WiFi issue is happening.

1. INTRODUCTION

Networks today have evolved significantly, one of the most tangible examples of this evolution are Wireless Networks. The most common way to access Internet from home are home WLANs, usually referred as home WiFi. The variety of services and devices using the home WiFi to access Internet is vast. It is common today for a home user to stream a movie on his laptop while connected to the home WiFi. In the ideal case scenario the experience is enjoyable, video team plays smoothly. In many cases, when the movie streaming is degraded, the experience is frustrating. One of the potential causes of poor streaming experience is the home WiFi. In fact, previous works [8] have identified home WLANs as the bottleneck along the service path. The cause of poor Home WLAN experience can be varied, as described in previous work [5], channel congestion, poor client or AP placement and interference are the most common causes. Other works [6] have analyzed the impact of Home WLAN on latency along a network path. They have identified that WiFi hops latency can contribute up to 60% of the overall round trip time along the service path. On top of these technical causes, a business risk arises. A risk between home users, ISPs and content providers. As described in previous works [1] the frustration is not only experienced by the users but also by users' ISPs who are often held responsible for poor Internet experience. This problem might seem small, nevertheless it can escalate until a point in which content providers lose their subscribers. Home users, in the search of a solution can switch between ISPs, if complication persists they can even switch content providers. In this context ISPs and content providers have little to none impact on one of the most common root causes of the degraded experience, the home WLAN. Under this light lies our motivation to develop a tool to identify Wireless impairments in Home WLANs. The description of the initial stages of this tool are presented along this paper. Identifying where the root cause is within the Home WLAN is challenging due to multiple factors. To begin with, Wireless nature is unreliable as it uses an open and shared medium, shared among WiFi and non-WiFi devices. Another factor is to choose the most suitable measurement technique to find where the problem is. At the time of this paper and to the best of our knowledge, most research works have mainly implemented passive techniques [3] [2]. A couple others have relied upon active techniques [4]. Depending on the type of measurement technique chosen challenges can be presented. Passive techniques face the challenge of requiring access to the device collecting the metrics. With active techniques the complication is tied to overhead caused by the measurement tool. In other words, with active techniques the very same measurement instrument can bias the measured metrics. Our tool implements a mixture of both to take strong points of both and leverage the weakness with each other's strong points. Further description of these techniques along with related work associated to home WLAN study will be covered in section 2. The instrumentation details of our tool are developed in section 3. The mechanisms and techniques to evaluate our method to identify impairments in Home WLANs is explained in section 4. Finally findings of our work are consolidated

in section 5.

2. BACKGROUND AND RELATED WORK

In this section we present a *high level overview* of what has been done with regards to Home WiFi problems identification.

We present the two methods for network measurements, active and passive. We describe the main characteristics of each of them and list the pros and cons of each one.

2.1 Wireless Monitoring Metrics

In the networking context and, to be more specific, in the network measurement context two techniques are well-known. These two techniques are **active** and **passive**. In one hand passive techniques "sit and listen" within the network whereas active ones "inject" traffic to fetch indicators about the status of the network. In the context of our work associated to identifying home WiFi issues previous works [3] [2] have chosen for passive techniques. In fact most of previous works have mainly focused on passive techniques. This might be associated to the granularity of data collected with passive techniques without adding overhead in the network. Some other works [4] have implemented active techniques. With active techniques the measurement are almost real-time. The downside is the risk of adding significant overhead to the network which might results in biased results. Each one of them has its own strong points and opportunity areas. In the following lines we outline the main characteristics of each one of them and what can be considered their pros and cons. Important to mention, we do not take any preference for one over the other. Each of the approaches will be best suited depending on the experiment goal and context.

Active

Active measurement techniques are mainly characterized by its ability to capture the state of the network in almost real-time. In other words, active measurement can help to identify a condition when is present in the network. This characteristic is different from passive network which can be considered historical. Active measurements are also characterized by the use of probes. Probe packet are used to measure the state of the network. For example, ping, relies on ICMP request and replies to compute the Round-Trip Time from one host to another. An important consideration to bear in mind when using active measurement techniques are the probes. It is important to define the size of the probes and how frequent are they sent into the network. Probes can add overhead to the network if their size is high compared to the capacity of the path or if they are sent too frequent. If probing is causing overhead to the network, the condition we want to measure will be caused by the same tool we are using to measure. Probing without the proper due diligence can lead to network degradation and/or biased measurements. In the following bullet points we outline the pros and cons of active measurement techniques.

Pros

- Full ownership of the network is not required.
- They do not require large space to store data collected as generally, probe packets are small.
- Privacy concerns are minimal as probe packet used to measure are made of random data which has no sensitive information.
- Useful to get the state of the network in real-time.

Cons

- They add overhead to the network as probe traffic is generated to conduct measurements.
- The very same probe packets being used to measure network conditions can cause network degradation.
- Biased results can be obtained if probing is conducted without due diligence of network conditions.
- They can only capture an instant of the network condition. If problem to be characterized is extended in time, active measurement might not measure it accurately.

Active Metrics

- **Round Trip Time**
  - This metric takes into account the time it takes for a probe to leave the source, reach the destination and come back to the source.
- **Throughput**
  - The amount of data that can be sent or received from or by a station will allow to identify how far are we from the PHY data rate. In practice the bandwidth is less than the PHY rate at which the station has connected to in 802.11 protocol PHY rate.
  - In other words this measurement can help to identify how efficiently is the medium being used.
- **Losses**
  - Losses from Ping statistic will allow us to identify the rate loss during the experiment window.

Passive

Passive measurement techniques rely on a listening approach. The instrument conducting passive measurements in the network sits in a specific location along the path and records the metrics of interest. The instrument can be a component of then network itself, like a router, or can be a device devoted to measure, like a Wireless sniffer. An important different between active and passive techniques, is that passive tend to be historical. In an historical sense, passive measurements are more reliable to characterize a network problem which cover an extended time-frame. Active measurements are suitable to pinpoint a problem in the instant it happens, nevertheless they lack accuracy to characterize problems which cover and extended timeframe. Another difference with active measurements is that passive measurements do not trigger probes. Overhead within the network path caused by probe packets is not present with active measurement. When implementing passive measurements it is important to consider the resources of the measuring device. The device might require to have enough storage to store the data being collected. In a similar way, the computing capability of the device an be required to be high depending on the speed of the link being measured. A Gigabit link in a Core Router will produce significantly more data than an 100Mbps Ethernet link of an access switch. In our tool we have passive tools such implemented Wireless Sniffer and WiFi metrics collection from Wireless client and Access Point. Outlined in the following list a high level summary of the Pros and Cons of passive measurement techniques.

Pros

- No extra traffic is generated to collect metrics, risk of causing overhead is minimized.
- They are better suited to accurately characterize network problems which cover an extended time frame.
- In general they are able to collect large dataset leading to increased accuracy of network complications.

Cons

- Data collected by them can be large. Large storage can be required to store data collected.
- Access to devices within the network is required in order to place the passive instrument.
- Measuring device might require to have computational power depending on the link being monitored and the granularity of data pursued.
- They are reactive, findings of network problem can be obtained after data has been analyzed.

Passive Metrics

- **RSSI - Received Signal Strength Indicator**
  - The power at which the signal is being received by the device. Depending on the type of traffic specific RSSI thresholds are often defined to define where the lower bound is located. For example, for VoIP the min RSSI value for an acceptable VoIP call is -68 dBm. In the other hand an RSSI -40 dBm is expected to deliver a good VoIP experience.
- **Busy Time**
  - This metric is associated to the time the channel was busy, in other words the time channel was being used and therefore not eligible for data exchange. Reasons for channel busy time to be close to 100% can be contention by other Wi-Fi devices or interference from non-Wi-Fi sources.
- **PHY Tx Rate**
  - The rate at which without medium access control, error correction or scheduling events the device is expected to operate with.
- **Frame Delivery Ratio**
  - Frame Delivery Ratio depicts the ratio between packets successfully received and total packet sent. The FDR metric can assist to get a sense of link quality. If FDR ratio is high then, the quality of the link can be perceived as good.

2.2 Where do we collect them?

We list the different vantage points from where the metrics have been collected in our work. We describe the reason of collecting them at the specific vantage point. For example, a characteristic to strive for is accuracy. Getting RSSI from client A will be different from client B, even if they are located at a similar distance from AP. The difference can rely on NIC, OS, firmware, driver, etc.

- **Bandwidth or Throughput** - We will measure it from the client as it is from the user that we want to get a sense of his experience. It is know that even with similar Wireless conditions devices can experience different bandwidth and bitrate. [7]. Therefore we will measure bandwidth from the client perspective at not from the AP. Measuring from the AP will give us a sense of the AP perspective and not from the client which is the device

from which the users access services. This metric is to be obtained using iPerf with UDP traffic.

- **PHY Tx Rate** - We will extract this metric from WiFi metrics at AP to identify at which rate was the frame being received sent. This correlates to identify the actual bit rate at which each frame is being sent. Metric is to be obtained from AP running Linux-based OS with the command *iwconfig*. We have also added a wireless sniffer to collect packet captures of the traffic between wireless client and AP.

- **RSSI** - Measure to be collected at the wireless client. The RSSI varies on wireless client location and obstacles in the path from Wireless client to AP. Metric is to be obtained from Linux-based client with the command *iwconfig*.

- **Noise** - A factor contributing to Wireless degradation is Noise, it is the Wireless interference coming from non-Wi-Fi sources. This can be caused by Microwave ovens, cordless phones and similar devices which "do not speak Wi-Fi language". Noise will be measured at both ends, client and AP as we strive to identify which one experience the more and less noise to pinpoint where the complication might rely. Poor AP or client placement. Command *cat /proc/net/wireless*.

- **Busy Time** - We will measure it from the AP as it is the one servicing clients in a specific channel (channels), meaning that clients will be connecting to that serving channel. If the busy time of the channel is high, means there is interference or other AP and clients using the same channel. A corrective action can be switching to a less busy channel. The busy time is made of two components, WiFi (congestion) and non-Wi-Fi (interference). Command *iw INTERFACE survey dump*

3. WIRELESS BOTTLENECK DETECTOR

In this section we describe the tool we have created.

It is a *custom* version of Ping in *GoLang*. This custom version allow us to define a probing rate, send probes in batches and set an inter-space between probes and batches.

Explain we have used exponential distribution to send batches. We have chosen exponential as Poisson process is related to exponential arrival times. We chose Poisson because sampling a Poisson process results in Poisson process, which allows to keep the same Poisson process even after sampling.

The sampling technique we used is Bernoulli, which is a type of Poisson sampling. In Bernoulli sampling all the observation in the data set have the same probability to become or not to become part of the resulting sampling set.

We varied the probability to be part of the sampling from 10% to 90%. To choose the sample which resembles the most to our original data set we worked with *Two Sample Kolmogorov-Smirnov* Test

Main characteristics of Ping Tool.

- The ping tool being used has been customized to be able to send batches of pings.

- The tool allows to define a probing rate based on a Poisson process, exponential distribution. We have chosen a Poisson process as we sample from it. Sampling from a Poisson process leads to another Poisson process.

- Our sampling rate has been defined to be 200 msec based on sampling and similarity test results.

Based on the similarity test conducted the rate at which batches will be sent has been defined to 200msec. Each 200msec a batch of 3 pings will be send, from the 3rd ping we will extract the RTT. We have chosen the 3rd ping as we found to be the one preventing the case of sleeping NIC, the first two ping were experiencing higher RTT due to sleeping NIC case. We tested this case in our lab by disabling power save mode in the Wireless NIC and noticing RTT went down for the first two pings. The case of sleeping NIC is often avoided with ping rate lower than 100msec, i.e. 90, 80, 50 msec. To validate our sampling rate, 200msec still holds in our testbed we conducted tests. The tests consisted in sending as many batches as possible for 10 min at 100 and 200msec. Additionally we varied the attenuation from 0, 15 and 30 dBm. The test sessions were conducted in the 2.4 GHz band using and 802.11n WLAN with no authentication. Each of the experiments was conducted 5 times, in total we obtained 30 samples.

Attenuation	Rate
0 dBm	100msec
0 dBm	200msec
15 dBm	100msec
15 dBm	200msec
30 dBm	100msec
30 dBm	200msec

To validate the similarity between the rates we compared the ECDF of each one, the curves must resemble to each other. In our case the results between 100 and 200 msec rate are depicted in the following images. In figure 1 it can be perceived similarity between two rates.

Figure 2 help us to validate an expected behavior. As we increase attenuation, the RTT is expected to be higher. This behavior is depicted in figure 2.

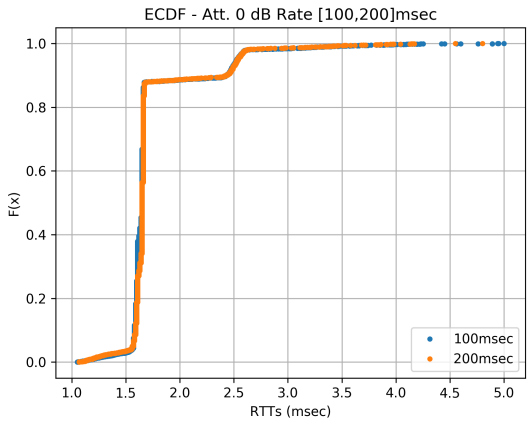

Figure 1: Att. 0 dBm - Rate 100,200 msec

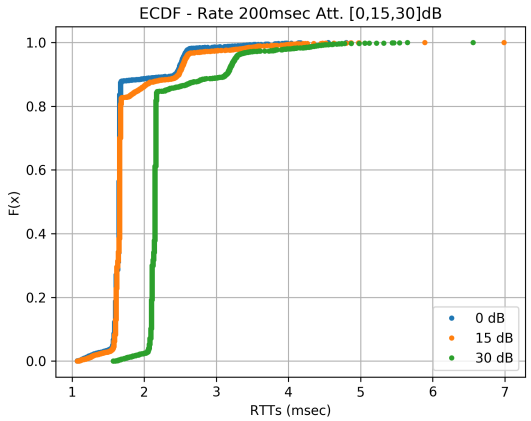

Figure 2: Rate 200 msec - Att. [0,15,30] dB

We can also describe that the p-value is close to 1 and the D-Value, which is the KS statistic is low. KS Low value is pursed as it means distance between the two ECDFs is small, meaning they are close to each other, hence more similar.

4. EVALUATION METHOD

Note: Ask on this section, as we might have already described it in the previous section.

4.1 Setup

Here we describe the setup we have in our lab and the test bed we have used in Orbit.

We have worked with two setup, initially our office lab and then Orbit.

In-lab

In our lab we have worked with a Raspberry Pi 3 running Raspbian GNU/Linux 8 (jessie). Wireless Access Point TP-Link AC1750. Dell Laptop Inspiron with Wireless Driver – *Driver Version* List Protocols supported by the Wireless card 802.11 a/b/g/n/ac Laptop running Ubuntu 16.04.4 LTS (Xenial Xerus)

Orbit

Main ideas for Orbit test bed description

1. Orbit is a testbed mostly devoted to Wireless experiments. (Mostly as they also have SDN sandboxes to test SDN technologies)
2. We have been using the Sandbox 4, SB4, which is devoted to Wi-Fi and Wi-Max Experiments.
3. SB4 is made of 9 nodes, each of them runs Linux based systems, Ubuntu 12.04 to be precise.
4. Our main setup is composed by three nodes. One node plays the role of the AP, another the role of Wireless client and the last one is a Wired client.
5. We are using 802.11n in 2.4GHz band to improve the reachability of the AP and the Wireless client.
6. The wired client is the source of the probes and iPerf server.
7. Wireless client plays the role of iPerf client.
8. We can include a diagram of the Orbit SB4 deployment and include the proper references.

Main ideas for the evaluation methods

- **Attenuation**
  - We have been using the embedded manger for attenuation in Orbit.
  - We can instrument attenuation values on the links connecting the nodes, in our case we vary the attenuation values between Wireless client and AP.
  - Attenuation controller allows to define values in the range from 0 - 30 dBm.
  - For our experiment we have been varying the values from 0 to 30 in steps of 3.
  - We vary the attenuation and record the RTTs for pings.
  - We have identified that after 27 dBm of attenuation is when we begin to see an increase in RTTs, each session last 10 min. Probe rate every 200msec.
  - At 30 dBm the connectivity between Wireless client and AP is lost.
  - For bandwidth test we have run iPerf and recorded the bandwidth obtained at the client side.

  - **With 5GHz we identified that after 6dBm the connectivity between client and AP is lost.**
  - We have setup 802.11n using 2.4GHz band to increase the range.
  - The goal is to run iPerf and identify at which attenuation levels does the bitrates drops, record the attenuation values to run ping tests.
  - Once the attenuation values have been identified the next step is to run ping tests using the attenuation values found with iPerf test and record the average RTTs.

- **Interference**
  - Currently looking for a way to create Noise in SB4.
  - Check if for a specific time they can setup a Microwave oven or similar.

- Congestion
  - For this experiment we will deploy a second wireless client connected to the same AP.
  - The 2nd Wireless client will send traffic to the iPerf server located in the wired client.
  - The original client will continue to send pings to the wired client.
  - We will record the results of RTT while other client is sending traffic to the iPerf Server.

We used three nodes with. Atheros 9k and 5k wireless cards.

We configure a node to work as a Wireless station, another as an AP and finally a third one as a wired client from where the pings were issued.

The third node working as a wired client plays a similar role as the Pi in our In-lab setup.

4.2 Setup of testbed

Here we explain how we ran the experiments.

We can set a "cost" to our experiments based on overhead at the following points.

- Network
- Device
- Router

4.3 RSSI in the wild

In order to collect realistic metric from can be considered a common value of RSSI in the wild we ran survey to collect this metric. We asked our colleagues in our office to run a script from which's output we can extract the RSSI value. We obtained 760 samples metrics coming from different environment contexts, mainly home and offices. We found RSSI average value in the wild to range between -60 and -60 [dBm]. Following picture depicts the histogram of RSSI obtained from the survey.

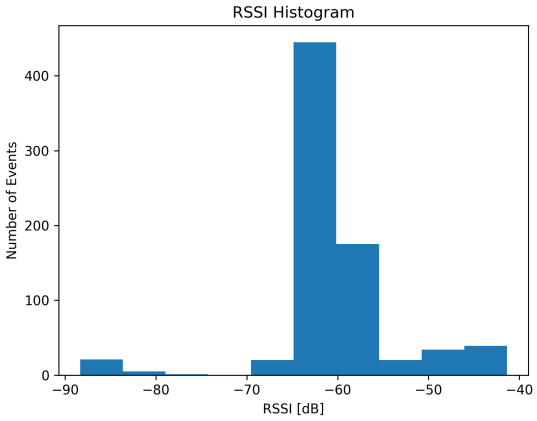

Figure 3: RSSI Survey Values Histogram

The main goal of this exercise is setup our testbed attenuation settings to trigger an RSSI value similar to the one found with the survey. In our testbed the attenuation values which lead to an RSSI value between the found range are 0, 3 and 6 [dBm] in the 2.4 GHz band.

We can include the accuracy of our methods depending on where are we setting our Vantage point.ex

In our lab we placed the laptop and the Pi close to each other, a distance smaller than 5 m. We connected to the 5GHz band under 802.11n protocol.

The first set of experiments consisted in progressively adding TCP sessions. The goal was to perceive how was RTT changed with more TCP sessions. We expected to see an increase as more TCP session were added.

Results matched our expectation and saw an increase in average RTT as more TCP session were added.

Include plot in which we have the CDF of RTTs vs TCP Streams

The next set of experiments were ran with the goal of finding a suitable probing rate. The ideal case is to probe frequent enough to have a "good" sense of the network without adding overhead and disrupting the Wireless Network.

We issued pings in sessions of 10 min at a ping rate of 100msec, initially, we call this aggressive scenario. The rate was defined to be 100msec to set our baseline from which we derived our sampling to obtain a suitable probing rate. The main goal is to achieve a rate which is not as aggressive as probing every 100msec.

After completing our sample analysis, we define it to be 200msec and we proceed to run test in Orbit where we can modify parameters as attenuation.

Orbit lab allow to modify attenuation from 0 dB to 30

dB. We perceived an increase in average RTT and loss rate from 27dB to 29dB. (At 30 dB link is unusable).

The results are show in the following plots.

Include Plots with Avg RTTs and Loss Rate results from Orbit

5. RESULTS

In the closing section we summarize what we have achieved, similar to what we have discussed at the closing of the previous section, 4.

Based on the tool and the methodology we used we outline the results we obtained.

What are our results telling us?

Can we identify impairments from the chosen metrics?

Which of the two methods, active or passive, can be considered to best suit the detection of Wireless impairments?

Why is the chosen method more suitable?

Future Work can be mentioned to describe the integration of this work with the project with Princeton.

6. REFERENCES

[1] Diego Da Hora, Karel Van Doorselaer, Koen Van Oost, and Renata Teixeira. *Predicting the effect of home Wi-Fi quality on QoE*. PhD thesis, INRIA; Technicolor; Telecom ParisTech, 2018.

[2] Diego Neves da Hora, Karel Van Doorselaer, Koen Van Oost, Renata Teixeira, and Christophe Diot. Passive wi-fi link capacity estimation on commodity access points. In *Traffic Monitoring and Analysis Workshop (TMA) 2016*, 2016.

[3] Diana Joumblatt, Renata Teixeira, Jaideep Chandrashekar, and Nina Taft. Hostview: Annotating end-host performance measurements with user feedback. *ACM SIGMETRICS Performance Evaluation Review*, 38(3):43–48, 2011.

[4] Partha Kanuparthy, Constantine Dovrolis, Konstantina Papagiannaki, Srinivasan Seshan, and Peter Steenkiste. Can user-level probing detect and diagnose common home-wlan pathologies. *ACM SIGCOMM Computer Communication Review*, 42(1):7–15, 2012.

[5] Kyung-Hwa Kim, Hyunwoo Nam, and Henning Schulzrinne. Wislow: A wi-fi network performance troubleshooting tool for end users. In *INFOCOM*, pages 862–870, 2014.

[6] Changhua Pei, Youjian Zhao, Guo Chen, Ruming Tang, Yuan Meng, Minghua Ma, Ken Ling, and Dan Pei. Wifi can be the weakest link of round trip network latency in the wild. In *INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications, IEEE*, pages 1–9. IEEE, 2016.

[7] Srikanth Sundaresan, Nick Feamster, and Renata Teixeira. Measuring the performance of user traffic in home wireless networks. In *International Conference on Passive and Active Network Measurement*, pages 305–317. Springer, 2015.

[8] Srikanth Sundaresan, Nick Feamster, and Renata Teixeira. Home network or access link? locating last-mile downstream throughput bottlenecks. In *International Conference on Passive and Active Network Measurement*, pages 111–123. Springer, 2016.