Wireless Impairments Detector

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

ABSTRACT

Lorem ipsum

1. INTRODUCTION

Computer networks have evolved significantly in the last years resulting in different services available almost everywhere. One of the most tangible results are Wireless Networks which play an important role in several contexts; whether if in offices, stores or homes. The fast-paced evolution Wireless has had in the last years have allow it to make its way into homes, bringing with it, its advantages and challenges. In one of the most common scenarios of wireless at home, the user with his connected device streams a video or plays online; suddenly the video stops or the online game "lag" or disconnects. The user, completing ignoring what can be the cause gets frustrated and calls his ISP seeking for assistance *as he has a high bandwidth Internet access with it* . In this scope ISPs have limited or zero-visibility of what is happening inside the home Wireless Network. ISPs scope is limited to assist beyond the last-mile to which they have access to. Finally both, users and ISPs, get stuck in a loop as they both have face a limitation to find the cause of the issue.

Main Ideas for the Introduction - Tell a Story

1. Networks have evolved significantly.
2. Wireless Networks are tangible evidence of it.
3. Wireless Networks are available almost everywhere.
4. Wireless has made its way into homes, bringing its benefits and challenges.
5. Wireless Networks are complex because Wireless nature is unstable, is a share medium.
6. Even Wireless experts face challenges while troubleshooting issues.
7. User watches a video or plays on his Wireless devices and suddenly the video or application stops.
8. Users gets angry as he does not know what can be causing it.
9. The first reaction is to call their ISP seeking for a solution.
10. ISP check his side, settings are in order from his end.
11. Users states that there is clearly a problem and he wants help as he is paying for a good service.
12. ISP has limited view into what can be the cause inside the Home Networks.
13. Both ends get "stressed" as they both face limitations.
14. Users lack knowledge and tools to help him confirm his Home Wireless is the problem or not.
15. User, in the other hand, has access to the home Wireless Network.
16. ISP lack the visibility and tools to troubleshoot user's Home Wireless.
17. ISP, in the other hand, has the knowledge to identify what based on metrics if the Wireless Networks is the cause of the problem.
18. As a final result User might end up switching ISP or content provider.
19. Switching ISP or content provider would not be a final fix as they root cause can be located in the Home Wireless.

Motivation - Why do we want to create a Detector

1. To assist users to confirm if home Wireless is the root cause or not
2. To help ISP to have tools to identify if the home Wireless is the problem
3. To have a tool which provides evidence that there is a problem in the Home Wireless

Outcomes from creating the detector

1. To assist users to confirm if home Wireless is the root cause or not
2. If the tool provides evidence home Wireless i not the root cause they can go to their ISP and ask for assistance.
3. To help ISP to have tools to identify if the home Wireless is the problem
4. If the ISPs have the evidence Wireless is the problem, then they can instruct user that the root cause is within the Home Wireless.

In this section we tell the story of why are we working to address the question related to Wireless impairments.

The main goal is to be able to identify Wireless Impairment in the Home Wireless.

Why? - Because most of the times the bottle neck in an end-to-end communication tends to be the Home Wireless.

Users gets frustrated as they do not know how to approach the problem. In fact, even with wireless networks knowledge identifying the root cause can be challenging.

Our work will become part of a tool which strives to identify where the bottleneck in and end-to-end communication is. The tool is already deployed in the wild.

2. BACKGROUND AND RELATED WORK

In this section we present a *high level overview* of what has been done before with regards to Wireless conditions measurements.

We refer to literature and mention the methods and metrics collected from those methods to predict, infer or asses Wireless conditions.

2.1 Wireless Monitoring Metrics

Here we list the metrics found in literature and list them under the two families, active and passive.

Active

Active measurements most tangible characteristic relies on the injection of traffic in the context to be measured. The traffic injection is mostly composed by probe packets. In other words additional traffic is triggered in order to extract metrics from the setting to be evaluated.

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 as minimal as probe packet used to measure are made of random data which has no sensitive information.

Cons

- They add overhead to the network as probe traffic is generated to measure.
- The very same probe packets being used to measure the performance can cause degradation of the network leading to biased results.
- 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.
- The ping tool being used has been customized to be able to send trains of probes.
- The tool allows to define a probing rate based on a Poisson process, 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 200msec based on sampling and similarity test results.
- Bandwidth 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.

Passive

Passive measurements rely on a listening approach, the passive instrument sits in a location within the network and listens to the traffic.

Pros

- No extra traffic is generated to collect metrics.
- They are better suited to capture long-term behavior as they can listen for an extended time frame.
- Due their ability to collect more data, the accuracy of measurement is higher than active.
- They do not introduce contention

Cons

- Data collected by them can be large. Large storage can be required to store data collected from Passive measurements.
- Access to devices within the network is required in order to place the passive instrument.

Passive Metrics

- Bit Rate The speed at which the device is connected to. Bitrate adaptation techniques are triggered based on channel conditions. Therefore this metric can assist to estimate the channel conditions.
- RSSI - Received Signal Strength Indicator The power at which the signal is being received by the device. Depending on the the type of traffic specific threshold can be defined for it. For example, for VoIP the min value for it is -68 dBm. What is consider a strong signal level is -40 dBm.
- Busy Time This metric tell us how busy was the channel, in other words if the channel the device is working on is close to 100% it can be due to contention by other Wi-Fi devices or interference from non-Wi-Fi sources.
- PHY Tx Rate (Bit Rate) The rate at which without medium access control, error correction or scheduling events the device is expected to operate with. As described before the PHY rate is higher than the bandwidth. *The PHY rate can be obtained from a radio tap, checking the 802.11 header and check the precise bit rate at which that specific frame was transmitted.*

2.2 Where do we collect them?

We list the different vantage points from where the metrics have been collected. We can also include the accuracy.

Note - From what I recall most of metrics have been collected from APs, which means we need to have access to the AP.

- Station
- Access Point
- Server

3. WIRELESS BOTTLENECK DETECTOR

In this section we describe the tool we have created.

It is a *custom* version of Ping in *GoLang*. This customer 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

Our results are:

Include chart with the results of similarity test.

In the plot we can see that with a probability of 50% we overlap our original data set.

Include Plot of ECDF of original data set and sample

We chose 50% as it results on an overlap with the original data set.

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

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 Evaluation method

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

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.