Towards Detecting and Reducing Unnecessary Active Scans in WLANs

Dheryta Jaisinghani
IIIT-Delhi
New Delhi, India
dherytaj@iiitd.ac.in

Vinayak Naik
IIIT-Delhi
New Delhi, India
naik@iiitd.ac.in

Sanjit K. Kaul
IIIT-Delhi
New Delhi, India
skkaul@iiitd.ac.in

Rajesh Balan
SMU
Singapore
rajesh@smu.edu.sg

Sumit Roy
University of Washington
Seattle, WA
roy@ee.washington.edu

***Abstract*—WiFi clients discover APs in their vicinity with the process of active scanning during which they inject low bit-rate and high power probe traffic–the requests and the responses. We show that clients trigger these scans without considering a need for it; thereby consuming airtime and reducing network goodput. This problem prevalent in heavily utilized WLANs. In this work, we begin with analyzing the effects of unnecessary active scans on the client-side and the network-wide scale. We provide a metric to measure the growth of probe traffic. We analyze the causes that trigger such scans and provide a device-agnostic solution to infer these causes at the network-wide scale. Finally, we develop a client-agnostic solution to reduce the number of active scans, by disabling them when not required. All our results are based on production WLANs.**

I. Introduction

Excessive and unnecessary active scans degrade the performance of heavily utilized WLANs. We find when the channels are at least 50% utilized, the amount of probe traffic grows up to 50% of the total management traffic, which brings down the network goodput exponentially [1]. Lesser number of non-overlapping channels and low bit-rate traffic aggravate the problem. The growth of this slow traffic beyond a certain point results in wasting significant airtime and performance drop. Network designers of production WLANs do not foresee this problem and hence, this is not a consideration. However, the performance of real-time and time-critical network services like VoIP is bound to suffer from excessive low rate control traffic. Furthermore, we find this problem is more prevalent in 2.4 GHz than 5 GHz. Developing countries like India are still at 2.4 GHz. Even the emerging large-scale IoT deployments will consider 2.4 GHz for price and range considerations. Latest standard update meetings also acknowledge this as an important problem to be solved.

Research Questions Q1. What is the extent and the impact of unnecessary active scans in heavily utilized WLANs?, Q2. How to detect the growth of probe traffic?, Q3. Can we detect the causes of active scanning at a network-wide scale?, Q4. Is it possible to develop a client-agnostic solution to reduce unnecessary active scans?

Research Challenges (1) Given the scale of clients and the traffic generated in large-scale production WLANs, detecting the exact cause of performance drop is hard. (2) Algorithms for active scanning are not only vendor specific, but they have multiple trigger points (Userspace, Kernel, or Hardware) at the client-side. This not only makes the cause detection hard but developing a device-agnostic solution challenging. Furthermore, client-specific solutions to reduce active scans cannot be deployed in production WLANs.

II. Work Done

Methodology [2] We follow an empirical approach. Multiple sniffers collect WiFi traffic, which is analyzed for the various metrics such as ACK losses, inter-frame arrival times, airtime utilization etc.

Q1. Extent and Impact of Active Scans [Under Review at TMC] We analyze two production WLANs with several thousands of clients. Our significant findings are that the stationary clients in 5 GHz scan 1.65 times lesser than in 2.4 GHz. Active scanning results in 91 times higher latency at the client. Even after discovering many APs with frequent scans, clients associate to same APs; that results in about 90% redundant probe traffic. When channels are at least 50% utilized, unnecessary and redundant probe traffic severely reduces network goodput.

Q2. Metric P/D [1] We develop a metric–ratio of probe traffic to fresh data frames. We show that cumulative growth of this metric allows detection of increasing probe traffic in real-time.

Q3. Active Scanning Cause Detection [3] We present seven causes of active scanning under three major categories–*Discovery, Connection Establishment, and Connection Maintenance*. We develop a sniffer-based inference mechanism to detect these causes at a network-wide scale. Our approach is device-agnostic and infers most causes with $F - Score$ accuracy of at least 0.57.

Q4. Client Agnostic Solution to Reduce Active Scans[Under Review at TMC] We develop a client-agnostic mechanism to reduce unnecessary active scans. It can be rolled out on devices as a simple application update. We propose to choose the need for an active scan dynamically. Our real-world analysis reveals an overall reduction of about 50requests.

References

[1] D. Jaisinghani, V. Naik, S. K. Kaul, and S. Roy, "Realtime detection of degradation in wifi network's goodput due to probe traffic," ser. WinMEE, WiOPT '15.

[2] D. Jaisinghani, V. Naik, and S. Kaul, "Poster: Mechanisms for detecting and mitigating performance drop in large scale wifi networks," ser. MobiSys '16.

[3] D. Jaisinghani, V. Naik, S. K. Kaul, and S. Roy, "Sniffer-based inference of the causes of active scanning in wifi networks," ser. NCC '17.