WPI-CS-TR-WPI-CS-TR-18-02 April 2018

Peering into the Home Network

by

Alan Ritacco
Craig Wills

Computer Science
Technical Report
Series

WORCESTER POLYTECHNIC INSTITUTE

Computer Science Department
100 Institute Road, Worcester, Massachusetts 01609-2280

Abstract

Previous studies have examined networking software approaches running on PCs and hardware, but there has not been a study that specifically identifies software tools and their provided data targeted to Home Networking. We are interested in understanding the complexity of these tools, and the required expertise to execute and configure as well as impediments to participation. In this paper, we look to understand and compare measurement points (MPs), applications and expertise required across four tool approaches: Routers, Apps, Hardware, and Web/Scripting tools. We also examine the data of interest provided by each approach. We show that focusing on a broad range of approaches, data of interest, and tools allows us to create a new taxonomy of Home Networking functionality.

1 Introduction

Over the past twenty years, the most widespread approaches to network discovery and research of Home Networks (HNs) have been to leverage physical hardware platforms to scan, and determine network flow using measurement points (MPs). MPs are the nodes, devices, or software where measurements are made [68]. Using protocols such as INM [8], Cisco Discover Protocol (CDP) [15], neighborhood awareness networking (NaN) [8] and others, have been leveraged to understand networking aspects of HN. In this paper we review what information routers, software applications (Apps), customized hardware, and Web/Scripting-based tools can determine in HNs. Understanding how we can leverage these approaches provides researchers, and more importantly HN users, results around local and global norms, as well as configuration of HNs and a new taxonomy system of information.

We refer to 'Tools' as software and applications running on a device. Tools can provide a plethora of localized information by peering behind the HN router using several approaches, in an attempt to determine and characterize configurations. These approaches range from modified and un-modified routers, Apps and software tools, customized hardware, and Web tools; all which use active or passive techniques and applications while executing. These techniques include those that look to peer behind the HN router to understand layout, configuration, and historical norms of the HN. As part of this study we look to understand how these techniques compare in terms of pros and cons of research, user incentives and impediments, and data of interest to HN users. This review focuses on the following approaches (exclusively): HN routers, Mobile and PC Apps (running locally and in the HN environment that scan and analyze HN configurations), customized hardware residing in the network that is directly connected to the HN for analysis, and passive and active techniques used by Web and Scripting tools and which executes within the local HN environment. We have focused this review in these areas as they cover the range of hardware, customization, software, and active/passive techniques one can leverage for HN informational scanning, and also have had some review previously.

As a starting point, we examined HN usage and have found the following data points. A review from 2009 of HN usage, across the US, found that 63% of homes had broadband Internet connectivity, and 50% have a HN [27]. A recent PEW report from 2017 found that 73% of all homes now have broadband Internet connectivity, and most of these homes have a HN [62]. Projects such as How's My Network (HMN) [68] used a software approach to peer behind these HNs to understand devices, and characteristics of a HN using a low footprint and minimal impediment methodology to incentive end-users to participate. Other work in this area has focused on understanding and characterizing Internet access (bufferbloat) and device evaluation via a heavy-weight client [48][19], while other work focused on hardware approaches to understand HN configurations [44][7]. The work in these areas were primarily interested in local historical norms of information, and data gathering.

We examine data of interest that are part of the approaches we are interested in studying, along with the tools that classified within these approaches. The data of interest include: Throughput, Networking Characteristics, Health, and Historical Norms, as well as each underlying attribute. We have reviewed the data of interest that each of these Approaches support, so that we can classify what each of tools cannot, could do, and do. We also look to understand the differences these approaches provide in-terms of data collection and dissemination of information. We are focusing our review on these Approaches as they cover the range of hardware, customization, software

(applications), and active/passive techniques leveraged in typical HN studies.

As part of this study we are also interested in health of devices (are they operating under normal parameters), applications, and protocols. This includes the health of DNS, security and privacy of devices and local configurations. The attributes of health include tools that examine configurations, normal operation, as well as the security and local device privacy. As a noted, Apps running tools described in this review have implications in these areas for both the local and network users, including potentially users residing on the probed network; these concerns are typically in the form of security and privacy implications. As an example, a tool that determines network devices on a network has possible security and privacy implications as it can determine and potentially track local hardware (via MAC) and fingerprint services overtime. This data is readily available using the techniques we describe in this report. We have created a section around security, privacy and health to understand these impacts and the type of information gathered.

Our contribution to this area includes a taxonomy of tools that fall into the approaches studied (Routers, Apps, Hardware, and Web/Scripting) and data of interest, difficulty level (incentive and impediments), and data availability (historical norms). The new taxonomies provide a classification of models around approaches and incentives, impediments, Source, Customization, and historical norms, along with data of interest; where norms has had little to no research up to this point. We conjecture that understanding local and global norms provided help users, and researchers, recognize the importance of distributed data sources and provide the incentive needed for participation in studies. In addition, we conjecture that understanding difficulty of applications usage and data provided can be the impetus for users to participate in HN studies.

The rest of this paper is organized as follows: Section 2 outlines background and similar work; Section 3 describes the methodology used ; Section 4 provides details on the study; Section 5 provides a review of data of interest; Section 6 is a comparison of Approaches; and Sections 7 and 8 conclude with a summary and future work, respectively.

2 Background and Related Work

We provide background and a review of previous studies on the Approaches, Data of Interest, and networking as part of HNs. This includes approaches and data of interest that fall into commercial (pay for tools or advertised tools) and research tools, and we look to understand how they fit into the areas of security, privacy, health, and characteristics of devices in HNs.

2.1 Approaches

In this section, we provide background on approaches and data of interest we are looking to understand. This includes a review of studies on approaches (Routers, Apps, customized hardware, and Web and Scripting tools), again we refer to the applications or the software running on these approaches as ”Tools”.

2.1.1 Routers

The following is a summary of information a typical HN maintains or includes (minimally) as part of its execution. A HN router has full access to the network and can gather information directly

from Layer 0. A HN router can sniff traffic similar to apps running root privileges or a heavy weight application using Packet CAPturing (PCAP) libraries; note that PCAP requires root privileges to execute or a specific kernel and modules [70].

A router has full access to the network and devices that are plugged directly into the environment. Typically, a HN router saves the routing table that consists of: MAC address, the IP address that was assigned to your computer, and the lease time of your computer's IP address; it also stores user-configurable items as well (port forwarding, etc.) In addition, manufacturers are starting to create Mobile Apps that control router access so that users do not need to login to the router via a web browser. These Apps are still in the starting stage and provide local information with very little norm overview, and certainly do not provide a global purview of information. Routers need to have logging enabled to store even minimal information, and this setting can be disabled (in error) by users during setup. Deep packet inspection is not a feature routers typically support, out of the box, and need to be rooted with tools such as WRT-DD [18] or similar software to allow these types of features.

As routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow, there main purpose is that of flow-control. As an example, if more than one path is available to transmit data, the router is responsible for determining which path is the best path to route the information. The Function of a Router is to also act as protocol translators and bind dissimilar networks. Routers limit physical broadcast traffic as they operate at layer 3 of the OSI model [51]. Routers typically use either link state or hop count based routing protocols to determine the best path. The Role of a HN Router has not changed much over the past 20+ years and are still found to deal with layer three of the OSI model (network layer). This means the hardware device has full access to all devices flowing through its traffic control ports, but does little else for HN research, as found from [10][30].

A recent study on routers found that there is not much data stored on the router over time. However, different routers can and potentially does store different data. As an example, data consisting of the assigned IP address of the connected computer, the computer name (or nickname), the MAC address of the computer, and the total time that the devices have been connected to the router [69].

HN routers have similar properties where they serve up local network traffic, WiFi, and maintain lists of information about what is on the network. Hardware vendors differ on what they provide for information, but typically contain the following services: DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. As an example, a wireless router, embedded with the ASUS DDNS service and other DDNS services, also supports the mapping of hosts, ex: (showing client name, IP, MAC, and Interface type). The router provides network flow (netstat information, ping, traceroute, and name server lookups via command line tools). A router can and does provide information about the local HN, but does not (typically) have a purview into applications and types of tools running; these require a modified/rooted router boxes and expert knowledge of networking and IT infrastructure, as noted by [69].

Research using modified home router software and tools have been completed using the toolsets WRT-DD [18], and Tomato firmware and configurations (or similar). Research by [9] found that a user must have high level of domain knowledge to work in these challenging domains of rooted environments, and went on to claim that users with minimal experience should "stick with the stock router firmware." Other work in this area includes Bufferbloat analysis by [50], performance anal-

ysis of home routers [34], identifying lurkers in social networks [78], and throughput performance [40], where these service and activities have all been done at a local level. Other research using modified routers with WRT-DD (or similar tools [Tomato, etc.]) was research to help understand and control network flow, wireless access, and discovery [69][5][43][17].

Other studies of routers found that understanding the causal impact of the different performance metrics around network performance is the only quantitative way of making such trade-offs of providing valuable data [73]. This study showed that a range of routers provided the following information: system status (CPU, RAM, and logs), Wifi networks under its control (3G and 5G for example), and by using a rooted router and DD-WRT firmware allowed researchers to control the devices similar to a Linux box (as it is a Linux based firmware), and collect, modify, and accept/reject streams via a very terse command line interface, and scripting tools.

An example screen-short of information from a commodity and stock router can be seen in image 1, and includes the following information: Device type, Client canonical name, local RFC1918 IP address, MAC Address, TX/RX information, and amount of time on the network.

Internet	Icon	Clients Name	Clients IP Address	Clients MAC Address	Interface	Tx Rate (Mbps)	Rx Rate (Mbps)	Access time
		Lorex	192.168.1.20 Static	8C:E7:48:		-	-	-
		Xbox 360	192.168.1.23 DHCP	7C:ED:8D:	2.4 G	5.5	-	45:48:59
		android-4ee3d358f87ca97b	192.168.1.39 DHCP	02:0F:B5	2.4 G	175.5	-	03:03:31
		thecube	192.168.1.104 DHCP	38:60:77		-	-	-
		Printer Cannon MX430	192.168.1.133 DHCP	88:87:17	2.4 G	1	-	449:44:21
		Wendy's Cell	192.168.1.137 DHCP	9C:D9:17	2.4 G	72.2	1	00:09:24

Figure 1: Example screen shot of a router

2.1.2 Apps

What is an App? According to [65], the term Software Application first appeared in the early 1950s and a Software Application, or App, is a program or group of programs designed for end users [3] that executes on a device or piece of hardware.

Mobile App -
A mobile App, as described by [81] consists of a software program that is targeted for a specific hand-held or mobile device type, e.g. Android platform. Tools such as [11][41][49][57] provide security, password and threat prevention via a mobile App, and functionality for a specific niche or data of interest.

Java App -
A Java App or Java Applet is an application, which runs in the Java Virtual Machine, which interprets instructions and executes on the system (hardware) that the application resides on. A Java program executing in a native environment has full access to the system resources, depending upon user privileges of course. A Java Applet executes within a browser typically (or similar restrained environment) and depending upon the nature of the execution has limited access to the resources of the system and executes in a sandbox (similar to JavaScript code). In contrast, a signed Java Applet has a fuller set of access to the resource it is running on. Our previous study [68] on HNs dives into a methodology and framework using a signed Java Applet and had promising results.

Techniques Used by Apps -
The following are some of the popular techniques used in commercial and freely available tools. Commercial tools such as fing [28], are available via a mobile app and hardware to help understand device mapping and network layout via the hardware; an additional purchase of hardware and licenses are required for these features. Other commercial tools such as [55][85][86][33] provide users similar information as fing, where none of these tools provide historical global norms.

Custom and UNIX (and other OSs) networking tools such as netstat, NMAP, and similar have a high barrier to entry and include techniques such as [36], which requires dedicated hardware and in-depth system administration skills to operate. Approaches such as Kermit [14] and Microsofts HomeOS project [4][21][20](established in 2010, now defunct) have attempted to use software models which requires a dedicated PC to run on. As an example, the HomeOS project was built with the premise that the Home needs an Operating System this approach has been all but abandoned. Other examples of App approaches include Ph.D. thesis work from [92], which claims to have minimal impediment to operate, but requires customized hardware running on a PC and extensive networking knowledge to operate.

There have been studies that have attempted to understand the layout (sketch) of the HNs, such as [64][31], as well as HCI (human computer interaction) studies around which techniques are useful to determine devices and resources in HNs, which have been unsuccessful as they have not provided a context of availability. An example of this is the Kermit [13] study, which attempted to map HNs broadband connectivity. A review by Grinter, et al. [32] attempted to use surveys to understand how HNs are setup and had similar results as [31], which found that participants needed technical knowledge to diagnose and deal with networked technologies, and that they turned to friends and family for help. This message has been re-iterated by the study from [63] where they found that the promise of future applications rests on the ability of house-holders to manage the home network, something that our collective research shows has not become easier since the first reports of connecting computers to the Internet. Furthermore, a previous study by [66] found that home networking is nontrivial for even the most qualified, and contend that these problems will not disappear over time as the networking industry matures, but rather are due to structural usability flaws inherent in the design of existing network infrastructure, devices, and protocols [72]. A study by Yiakoumis, et al. [90] looked at extending this type of work and came up with the concept of slicing the home network in an attempt to understand the landscape of the HNs from an App and hardware perspective.

The dynamic adaptive streaming over HTTP (DASH) work and others in QOS (quality of service) and HN [47][77][76][83][91] have looked at performance of HN and content delivery, while

[12] looked at benefits of Software Defined Networking (SDN) to see how they can help improve manageability. Studies have approached HN review to include load time of objects to determine under-performing content [29], while others have used DASH to understand video streaming in HNs [46].

Commercial tools (pay to use and requires a license), such as [71][28][54][84][88][87][52], are available that help understand the presence of devices on the local network, security, privacy, or use Wifi to determine least crowded channels or discovery using Bluetooth, and provide little historical data for local configuration and global norms. While these techniques provide specific data sets around BufferlBloat, DASH, throughput, or point and time information, none of the tools reviewed provide historical global norms of HNs nor configurations of these HNs.

There are commercial apps that are available for both Droid and iPhone that can scan Wifi networks (similar to HMN), and determine open ports, but this area not well researched nor does it have available data sets for researchers to review. These Mobile Apps have limitations on accessing the TCP stack, and therefore cannot provide details that tools such as nmap (for the PC) can provide (active fingerprinting), noted by [45][61], and require elevated privileges to execute. The following are some Apps reviewed and are either commercial or research and are the most applicable in-terms of providing networking information:

- Netalyzr [48] provides information around Bufferbloat, which has been well studied, as well as general internet upload and download throughput.

- fing [28] is a mobile App which scans for local Wifi connected devices. An interesting feature is the Enable device recognition, which requires remote best-match brand/model of device, assumedly via Mac address. This is an opt-in request that the user must click Enable to allow access to the remote querying fingerpedia. This tool requires users to enter information about host, and can run a simple scan of open ports on the given host; it does not predict the type of host (ex: Linux RedHat, Microsoft Windows 10, etc.). Each scan is manual, and is required to be run explicitly by user requests [53]. There is an optional hardware device for lower layer analysis scanning and reporting.

- Mobile NMAP [56] provides similar information to the PC counterpart, but it limited in-terms of resulting scans (i.e. no OS fingerprinting, SYN scan, etc.). NMAP does not explicitly provide global norms, and requires a high level of knowledge and expertise to operate.

- Tools such as Wifi Analyzer, Wifi Master, and Wifi Connection provide Wifi channel information in an attempt to show the least crowded connection (channel) to the router [84][86][85]. These tools do not provide historical global norms, but may provide best practice information on management.

- Other tools such as Meshlium use Bluetooth and Wifi signals to identify devices in a given area; these are commercial products, which typically require a hefty up-front cost and monthly subscription, such as [52][58]. These tools are localized only and do not provide historical global norms.

- Rooted tools, such as from the review by [70], can provide a deeper view of things, but have a higher barrier to entry (requiring a fat client to be installed on a PC and customized

hardware) and are not targeted the novice user. These closed source tools do not provide global norms.

- There are other commercial and open Apps, which provide network scanning, Wifi, and upload and download information, but do not provide local and global norms nor provide the breadth of data across the range of spectrum users may be interested in.

Health and Apps -
There are several Apps which look to determine health (including security and privacy) by examining the local host (PC or Mobile) run time nature, and configurations. Tools such as [1][6][74][16][80][60] look to understand mobile and PC security around virus protection, remote theft, safe browsing, SMS, encryption, proxy, and tracking. These tools use virus definitions, GPS location services, phishing definitions, encryption techniques (such as twofish, blowfish, and others) to encrypt applications and text messages, as well as triangulation (using Wifi and GPS) for health, security, and privacy.

2.1.3 Customized Hardware

Customized hardware consists of devices packaged (or not) with an App [58][28], network security devices, IoT devices such as sensors, automation devices, and network devices modified to allow for access control [18]. These devices use pass through features and remove the HN router from the network [58], or act as the primary Wifi connection for the network, thus routing all packets through the customized box. These devices serve as active and passive monitoring for security and remediation, device look-up and traffic control on the HN. As an example [58] algorithms to pre-execute control techniques to traffic flow, in conjunction with cloud-based inspection. These hardware devices are either highly customized routers/Wifi units [58], or expensive commercial products [23][52] targeted for specific tasks (e.g. security, sensors, discovery, etc.)

Most research based hardware devices consist of modified routers, and software packages leveraging cloud-centric analysis. Commercial hardware approaches typically consist of devices packaged (or not) with an App [28][58], network security devices, IoT devices such as sensors, automation devices, and network devices modified to allow for access control [18]. These devices use pass through features and look to remove the HN router from the network and act as the endpoint security connection or as the primary Wifi connection for the network; thus routing all packets through the customized box. These devices serve as active and passive monitoring for security and remediation, device look-up and traffic control on the HN. Each of the following hardware solutions require a monthly subscription to leverage security and privacy features, and thus have a barrier to entry.

- Bitfender [58] uses machine-learning algorithms to pre-execute control techniques to traffic flow, in conjunction with cloud-based inspection. The hardware is highly customized router/Wifi unit [84] and requires an additional hardware unit to replace HN units along with a monthly subscription [24][52] targeted for specific tasks (e.g. security, sensors, discovery, etc.). This device does not provide global norms.

- Cujo [25] is an inline device plumed into the Ethernet of the HN. The device monitors traffic for security threats, and looks to prevent sensitive data from leaving the HN. It is not clear

if this devices require a switch that mirrors all ports to gather data, as it is plugged directly into the HN router. The device does not provide global norms.

- Dojo [22] is also plugged directly into the HN via a port on the router, but examines metadata versus full stream to determine actions. It is also not clear if this devices require a switch that mirrors all ports to gather data, as it is plugged directly into the HN router. The device does not provide global norms.

- Keezel [42] connects to the network purely via Wifi, acting as a hotspot and flow through using VPN based technology. This device does not protect hardwired devices (unless direct mirroring is created on the router), and does not provide global norms.

- RaTTrap [67] is directly plugged into the HN modem, and the HN router is plugged into the device. This allows the device to examine all network flow inbound and outbound and it looks to block malware and other security threats.

- We also list Fing [28] device in this section as it is provided either as a software or hardware/software solution. As previously mentioned the FING tool does not provide distributed data from global norms, as it is a commercial closed App/hardware tool.

2.1.4 Web Apps and Scripting Tools

Tools running in a web browser and scripting tools, such as JavaScript, HTML, Python, and other similar languages are not required to be complied and are strictly speaking interpreted [89]. These tools, when executed from a Web Browse or similar environment, run in a sandbox and are allowed minimal access to system level resources.

Web or Script based approaches leverage either a browser or command line interpreted tools such as Perl, PHP, HTML5, and shells such as BASH. As an example, these tools look to query for: hardware devices, software running locally, OS and security settings, Active Directory (AD) configurations and settings, local web service settings, and local user and group information. To gather much of this information they must be installed via administration/root privileges locally or the collected information is minimal when running via a web browser. It should also be noted that unless these tools are run directly within the HN they would only provide scanning information from the edge of the network, as they cannot peer inside the HN and behind the router remotely.

- Open-AudIT [82] was released in 2002 and is targeted at system administrators who have deep knowledge of Linux or Windows systems to just install. The tool when run as root can collect network information such as hosts, MAC information, and when configured with NMAP a deeper dive of devices using NMAP fingerprinting. This tool does not provide global norms, and can be a challenge to configure and run.

- Spiceworks [75] is a Web based port scanning tools, but can only determine edge information and cannot peer inside the HN.

- Pentest-tools provides TCP (and UDP) Port Scan with Nmap [79] via a web browser, and leverages the Nmap tool to collects data from their server running Nmap fat client. This tool does a minimal execution of Nmap or a bit more passive scanning. The tool leaks

information around the location of the server running the scan by listing the time zone and time of the scan in GMT time. This tool does not provide global norms.

- Mxtoolboxs [53] provides similar functionality as Open-Audit and runs an open TCP connection via port request to the edge device on the HN. This tool does not provide global norms.

- Hows My Network, predicating performance from within a Web browser sandbox [39] leveraged scripting tools run via a web browser for performance analysis in a HN.

2.2 Data of Interest

In this section we review data of interest and the attributes associated with each of these. The following are studies and other work that have done work similar to the data of interest we are most interested in. These tools determine the following high level of information as related to the approach and data of interest: Throughput, Networking Characteristics, Health, and Historical Norms. These data of interest individually provide a small amount of data, but tied together create a valuable picture of HNs and what is occurring in them.

2.2.1 Throughput

The area of throughput has had extensive studies in-terms of: Upload, Download, Jitter, Network Flow, and Performance. Studies such as [68][39][36][89] looked to classify upload, download and Jitter by calculating changes in network traffic and differentials of time. While [48] looked at network flow and jitter in-terms of bufferbloat and delta changes in traffic. Work done by [56][21][77] looked at local network performance of HNs to understand traffic flow and overall performance, other studies such as [73] looked to understand if performance matters in the HN. These and other studies provide background needed to tie together throughput of HNs to create a concrete picture of what is occurring in HNs.

2.2.2 Networking Characteristics

In the area of Networking Characteristics we are interested in the attributes such as: Device discovery, Network fingerprint, Wifi Network discovery (online and previously attached to). These areas help bring together a picture of devices, and activity occurring in HNs. Studies such as [68][56][28][55] and others provide device discovery and network fingerprinting by using well known broadcast services, TCP evaluation, and port mapping to evaluate devices available on a network. Wifi tools such as [86][84][85] and others provide similar analysis for Wifi networks to understand a mapping of Wifi, radio and communication channels, as well as historical information of devices attached and previously attached to a Wifi network.

2.2.3 Health

Health of networks, applications, and devices includes the following attributes: DNS, Apps, Security and Privacy (Apps, Location, Monitoring). Studies such as [68][56][35][38][26] looked to

understand 1st, 2nd, and 3rd tier DNS results, SOA requests, recursive requests, as well as security and a variety of approaches to health and the local and remote DNS services. Research into apps (running on PCs or Mobile devices) have looked into options of security and privacy [25][22][42][67] on local devices. While research and tools such as [58][2][23] look at hardening security and privacy of the device and the network. While some of these tools require expert knowledge of networking and security, others look to harden and quarantine network flow, file access, network access, and app access.

2.2.4 Historical Norms

As previously discussed Historical Norms provide information on: Local Norms, Global Norms. While most Apps and research provide local norms, there are only a few Apps or research projects that provide global data norms for users (and researchers) to understand a big picture of what is occurring across disparate HNs. As an example, the work done by [68][39] provides results of throughput and networking characteristics of both the local and global norms for comparison.

3 Methodology

In this section, we provide the methodology used as part of this review. We start with the methodology that was used in this tech report, and then turn to why this research matters and look to understand optimal setup and how a user or researcher can mimic this in a HN.

We reviewed research papers, tech reports, and commercial products and then compared the methods used, and results provided by the given work. We have classified these, and looked for overlap and similarities, differences of results, as well as the methods used to collect and display the information. This research included an unbiased review of the Approaches, Data of Interest, Historical Norms, data collection techniques, and results. From these results we turned our attention to what types of data results users and researchers are interested in and looked to combine these differing Approaches, Data of Interest and Historical Norms. The data of interest included data both currently collected and not currently collected by these works, along with how to display this data using different HCI approaches.

To understand the data of interest provided from these approaches we have download tools, reviewed papers, and dichotomized the results and methods of the App/tool. We looked at the results of these Apps/tools and include a data of interest set discovery and attributes, including: throughput, devices, health, security and privacy, along with historical norms.

In addition, we look to understand the incentives, and impediments to each approaches and classifications around the areas. Incentives and impediments are focused on the user experience and more importantly the perceived value of the tool and barriers to entry respectively. An Apps approach may be free to users, and require minimal impediment to install, configured, and execute and thus have a lower barrier to entry.

We have reviewed the following areas to understand why this research matters to the user and the research community. As previously mentioned, it is clear that the work done by commercial, discovery, and tech reports provide a clue to what users may be interested in. This includes the desirable areas of throughput, network characteristics, health, security and privacy, and most importantly how information collected compares at a local and global norms. An optimal setup for

users to execute this work would be a collation of the data of interest into an App, along with information gathered from historical norms. With that said, these approaches can be completed using physical (inline) hardware or via an App.

As mentioned, the method used by this study included an in-depth review of research papers, commercial and openly available applications/tools, underlying protocols, impediments and incentives, and a comparison across approaches and data of interest. We have examined a broad range of software and hardware as well as the Data of Interest that are part the Approaches that we are interested in. We first look to create a dictionary of terms and definitions for this study to clarify the method and have created the following definitions for this study, which include:

- Approaches: Hardware and software that provide a plethora of localized information by peering behind the HN router using several approaches, in an attempt to determine and characterize configurations. We refer to the Software/applications running on these devices as 'Tools'.
  - Routers:
    - Stock and Customized
  - Apps:
    - Mobile, Java, executable(s)/binaries
  - Hardware:
    - Customized hardware installed in the HN
  - Web/Scripting tools:
    - Software running within a web browser or via a scripting run-time
- Data of Interest: the gathering of desired data collection from the user perspective. We have included the attributes of each of these data of interest, which are the data points collected by the tools.
  - Throughput
    - Attributes: Upload, Download, Jitter, Network Flow, and Performance
  - Networking Characteristics
    - Attributes: Device discovery, Network fingerprint, Wifi Network discovery (online and previously attached to)
  - Health
    - Attributes: DNS, Apps, Security and Privacy (Apps, Location, Monitoring)
  - Historical Norms
    - Attributes: Local Norms, Global Norms

We used the following method to classify and understand the differences within and across each of these Approaches and Data of Interest. We compared each of the tools that execute across these Approaches and Data of Interest to understand the quality of information (high and low), incentives to execute (richness and quality of data), and impediments to entry (easiest to hardest).

We next extended these comparisons, uniformly, across each of the approaches and data of interest (grouped by approach and the Tools), and used the following system to help understand the data of interest of each of the Approaches.

- Cannot be done: The data of interest does not have the access to this type of information.
- Could be done: The data of interest can do this.
- Done: The data of interest is supported by an application within this approach.

A comparison was also completed by reviewing the set of tools (arraigned by Approach type) and comparing by the following measurement of approaches, data of interest, and tools: incentives vs. impediments, sources and customization vs. data collection set, and historical local norms and historical global norms. We used the following method to understand these three measurement comparisons and differences, and used the data sets compiled as part of this study. We refer to this as user participation data points.

We compared incentives and impediments to each other and created a classification of paradigms to understand easiest and best vs. the hardest and least ranked tools. The following was used to understand Incentives, and Impediments of each Tool and thus Approach.

User participation: The following are the comparison areas of user participation data points: incentives and impediments, sources and customization vs. data collection set, and historical local norms and historical global norms:

- Incentives and Impediments: incentives and impediments are focused on the user experience and more importantly the perceived value of the tool, and the barriers to entry.
  - Incentives:
    - None: No incentives are offered to participate in a study or are provided by the tool.
    - Low: Minimal amount incentives are offered by to participate in the study or information provide to operate the tool.
    - Medium: Incentives are offered that provide users a reason to want to participate or operate the tool.
    - High: There is a high amount of incentives offered to participate or the tool offers a wide range of information.
    - Impediments:
      - None: There are no impediments to operate or participate
      - Low: There are minimal impediments to entry
      - Medium: The impediment to entry is challenging and requires monetary or skill level to operate
      - High: Barrier to entry includes monetary or expertise to operate

We used the following for the comparisons of Sources and Customization vs Data Collections used the following classification.

- Sources and Customization: is the platform open or restricted in-terms of modifications and changes, including sources
  - Closed: No changes are allowed, and sources are not available.
  - Restricted: Minimal changes are available to the configuration or the sources
  - Open: A wide variety of configuration options are available to modify, and sources are available.
- Data Collection: the types of information provided by the given Approach/Data of Interest.
  - Restricted: A restricted view provides closed and minimal information
  - Flexible: A flexible view provides some modifications for request to wide range of information.
  - Open: An open view allows for low level modifications and access to configurations for customized set of information

Similarly, we reviewed and compared historical norms (local and global) in-terms of data sharing and availability, and used the following classifications for this comparison.

- Historical Norms: either local or global.
  - Local Norms: The types of data the tools provided at the local network level, and if there is a long range or a point and time comparison of this information.
    - Closed: Information is not provided by this tool
    - Restricted: Data is gathered over a given set of time, and provided to users for review. A limited amount of Information is typically provided by the nature of the product, and is typically point in time.
    - Open: Data is available on a wide variety of areas, and is flexible for types of information provided.
  - Global Norms: What, if any, information is provided, by the tools, for comparisons to users running these Applications at the global level, across networks and users. Data that is used to compare to other environments, which is running on the same Approach/Data of Interest type.
    - Closed: information is not provided by this tool.
    - Restricted: Data may be gathered, but is not provided for review.
    - Open: A wide range of information is available by this tool.

4 Approaches and Data of Interest

In this section, we organize approaches and data of interest by collections provided. We start by looking at how each of these approaches are tested and classified. We have created an approach taxonomy of routers, Apps, hardware, and Web and Scripting, as shown in tables[1,2,3,4].

These tables provide information around: approach, source, incentive and impediments, and historical norms. As part of the review of these areas we have also created four tables focused on approaches and data of interest, including what sources and customization, data collection, and historical norms they support. The tables provided show the measurement approaches that each of these areas cover, along with comparisons of like types. The objective of these tables are to help understand what types of information each approach provide (to users), along with incentives, impediments, as well as location and metrics. We use the classification shown earlier to describe these areas:

4.1 Routers

As previously discussed, routers can provide the richest set of information, but can require a high level of expertise to operate. Table 1 to show information around approaches, stock (out of the box) router and a customized rooted router, source, incentive, impediments, and historical norms.

- Source: both methods are closed, with the exception that the modified router has updated firmware which exposes additional functionality (e.g. custom control points).
- Location: both methods are targeted at home and commercial networks
- Incentive: a stock router provides access as its major incentive, versus a modified router that provides users, and researchers, to customize their networking experience and data collection points.
- Impediments: a stock router requires a medium level of expertise to install, and configure, as previously noted, and its major impediment is around cost of the unit. A modified router is also has the impediment of cost, but has the additional requirement of expertise to install, configure, and operate as it requires a high barrier to entry.
- Historical Norms
  - Local Norms: both methods provide local information about the network to users.
  - Global Norms: neither method provides information from other users experiences or feedback.

Table 1: Classification of Router Approaches, Tools, and Data of Interest

Router Tool Approaches				
Tool Type	Source	Incentive	Impediment	Historical Norms
Stock	Restricted	Access	Medium purchase	Local Only
Rooted	Restricted Modifications to firmware	Access Custom	Equipment Expertise	Local Only

4.2 Apps

We have created a similar comparison for Apps in Table 2 from the following:

- Source: HMN and Nmap platforms provide are available as open source
- Incentive: All of the platforms provide feedback as an incentive, with the exception of Fing which is driven as a pay for service and ad-driven tool.
- Impediment: A review of impediments across the platforms shows the following:
  - HMN, and Fing are the easiest to install and require the least amount of impediment to entry
  - Nmap and Kermit require administrative access to run and a PC and customization to run, and thus have a higher barrier to entry
- Historical Norms
  - Local Norms: all methods provide some information to the end user over a given set of time.
  - Global Norms: The HMN approaches is the only tool that provides both local and global norms for comparisons.

Table 2: Classification of Apps, Tools, and Data of Interest

Apps Measurement Approaches				
Tool Type	**Source**	**Incentive**	**Impediment**	**Historical Norms**
HMN Java	Open	Feedback	Medium Approve app	Local Global
HMN Mobile	Open	Feedback	Medium Install App	Local Global
nmap	Open	Feedback	High Expert	Local
Kermit	Restricted	Feedback	High Special HW Expert	Local
Fing	Restricted	Feedback via pay product	Medium Can require additional HW	Local
Netalyzr	Restricted	Feedback	Medium Install App	Local

4.3 Customized Hardware

We next turn our focus to devices that are directly attached to the HN and are specifically targeted around discovery services. As discussed these devices use similar methodologies as routers, as they are directly connected into the network with layer 0 level access. The information gathered ranges from device types, machine names, internal throughput and throttling controls, WiFi troubleshooting, and network security. These devices collect local information, but do not share local or global norms, and are classified as heavy-weight. Tools such as fing require a hardware device to be purchase to extend the information available on the network. These tools can leverage both software interfaces and hardware as they directly plugged into the main network (similar to the router) to determine device characteristics using similar approaches to that of Apps.

We have reviewed two approaches, as can be seen in Table 3, Fing Hardware, and HomeOS. Each of these approaches shown in Table 3 are classified as customized hardware, as they are specific to device scanning and HN tools. They are typically paired with software or run can be run directly via the hardware devices (Web Browser). Some key points of this include:

- Source: Fing and the HomeOs approaches are both restricted and do not provide open sources
- Incentive: Fing and HomeOS provide feedback as the major incentive, but both require custom hardware to run and a licenses is required from Fing to operate.
- Impediment: Fing and HomeOS provide device information, but the HomeOS tool looks to provide access and control of IoT based devices. Both methods have a high barrier to entry, as they require customized hardware to execute and a license to operate.
- Historical Norms
  - Fing and HomeOS both provide local norms over time.
  - Neither Fing nor HomeOS provide global norms of other (user) experiences.

Table 3: Classification of Customized Hardware Measurement Approaches

Customized Hardware Measurement Approaches				
Approach Type	**Source**	**Incentive**	**Impediment**	**Historical Norms**
Fing	Restricted	Feedback via pay product	Medium Require additional HW	Local
HomeOS	Restricted	Feedback	High Requires Custom HW	Local

4.4 Browser and Script Based Tools

Browser and scripting tools run directly within a web browser, and do not require the user to download tools to execute. The Barrier to entry is low for the end user to execute, but the tools provides minimal information during executions, due to the sandbox that it executes within. Tools such as speedtest [89][59] and [39] run within a web browser and use point locations (throughout the country or localized) to understand throughput and jitter to know resources.

Table 4 is a taxonomy of these approaches, and includes a review of generic speedtest services, and HMN sandbox methodologies. HMN is an open source approach to testing versus speedtest, and they are both targeted to HN and Commercial networks for testing. They both are free in nature and provide feedback and the major incentive, and require minimal impediment to execute via a Web browser. These approaches provide similar results, but HMN provides both local and global norms.

- Source: Speedtest tools are closed source versus HMN, which is open source and can easily be modified.
- Incentive: Both methods have the user incentive of feedback of information to execute, and are typically no cost to execute.
- Impediment: Both of these methods have the most minimal of impediments to execute, but provide the least amount of information due to the nature of how and where they execute, e.g. via a web browser.
- Historical Norms
  - LocalNorms: Speedtest services provide point and time executions vs. that of HMN which can provide a comparison based off of previous tests.
  - Global Norms: neither method provides global norms, but the HMN suite does provide the ability to understand longitudinal information from the data gathered.

Table 4: Classification of Web and Script Measurement Approaches

Web and Script Measurement Approaches				
Approach Type	**Source**	**Incentive**	**Impediment**	**Historical Norms**
Speedtest Services	Restricted	Feedback	Low Minimal info	Local
HMN Sandbox	Restricted	Feedback	Low Minimal info	Local

5 Data of Interest

The following is a review of each of the data of interest and tools reviewed in this study, along with the merits in their own area. These merits are classified at the Approach level, and include the following:

- The router approach allows for the customization of information, but requires a high technical barrier to entry for customization. Data that is gathered is point-in-time and is typically cycled over X number of days, but is not made available in a longitudinal approach to users or researchers.
  - A stock router is a utility approach to computing, and networking as its main focus is access versus information.
  - A modified router can provide the deepest dive of information from method of approaches studied. This approach can provide information ranging from performance to information, but as previously discussed has a high barrier to entry.
- The Apps approach is the most flexible as it requires the least amount of efforts to entry for the user, and can be customized to allow for both practical user, research and technical information, without the use of hardware. With an App, users have the ability to understand data for global and local norm comparisons. This is important as an App can be customized and include a Human Readable Format, including:
  - Device list
  - Throughput (Up/Down), jitter, etc.
  - Performance of the Device
    - Legacy information about the devices attached previously (assumed it was scanned)
    - Device was present, or is now present, and is now gone
  - What is shown and how it is shown, over time.
  - Apps provide methods to push updates to devices (e.g. phones), with minimal impediment to end-users.
  - Apps can flexibly be customized in-terms of configuration and results to an end-users perspective.
  - Apps can provide devices and configuration of networks, in a local and global approach.
  - Apps provide and understanding of protocols and configurations of these domains.
  - Apps also have information with activations and Activity of the HN and the device running scans.
- Hardware measurement approaches can have similar success as a modified router method, as they have the ability to sit inline of the router, and can analyze data in a similar manner that a router. These devices serve a specific function, and have a license and cost as a barrier of entry. While the nature of these services are to minimize impediments, they have a high barrier to entry and are tech savvy approaches. Information gathered from these approaches are quite specific, and are targeted at a specific product approach. Data collection in these approaches are targeted, and provide feedback to the local vs global instance only.

- Web and Script Measurement approaches have the least impediment for barrier to entry as they can run via a web browser, or similar. They provide minimal information in-terms of data discovery, as compared to the other approaches, and only provide a local point-in-time data set.

We next turn our attention to the comparison of approaches and what types of results, device characteristics, platforms, components, and services they fall into. The classifications of user participation in-terms of what can be discovered using a Router, commercial tools, and other hardware devices is shown in Tables 1,2,3, and 4. These tables look to understand how they fit into the data of interest. The tables provide information around the following classification areas that are the most important as shown from the work reviewed, and previous studies. We are looking to understand the following data points and sub-items, as they appear to be the most commonly studied across the set of tools and research papers reviewed.

- Throughput
- Network Characteristic
- Health
- Historical Norms

5.1 Throughput

We have created a classification of information that each approach type collects in-terms of throughput. We have classified throughput to include the following characteristics of the areas we are reviewing (routers, Apps, Customized Hardware, and Web and Scripting tools), and includes the following:

- Internet and local network Upload and Download: Throughput of the Internet connection and internal throughput.
- Jitter: Deviation from optimal performance of a given Internet connection or the fluctuation of latency over time, and includes ping spikes and lag.
- Network Flow Diagnostic of network layers, including TCP flow.
- Performance of Device (perf) Diagnostic information around the performance of devices attached to the network.

We can see from Figure 2, that a variety of information can be gathered using each of these approaches, and that the Apps approach has at least one tool in the list that provides this data set.

5.2 Customized Hardware

Table 1 provides a review of network characteristics against the approaches we are reviewing. These include the following networking areas of review, and what information can be collected.

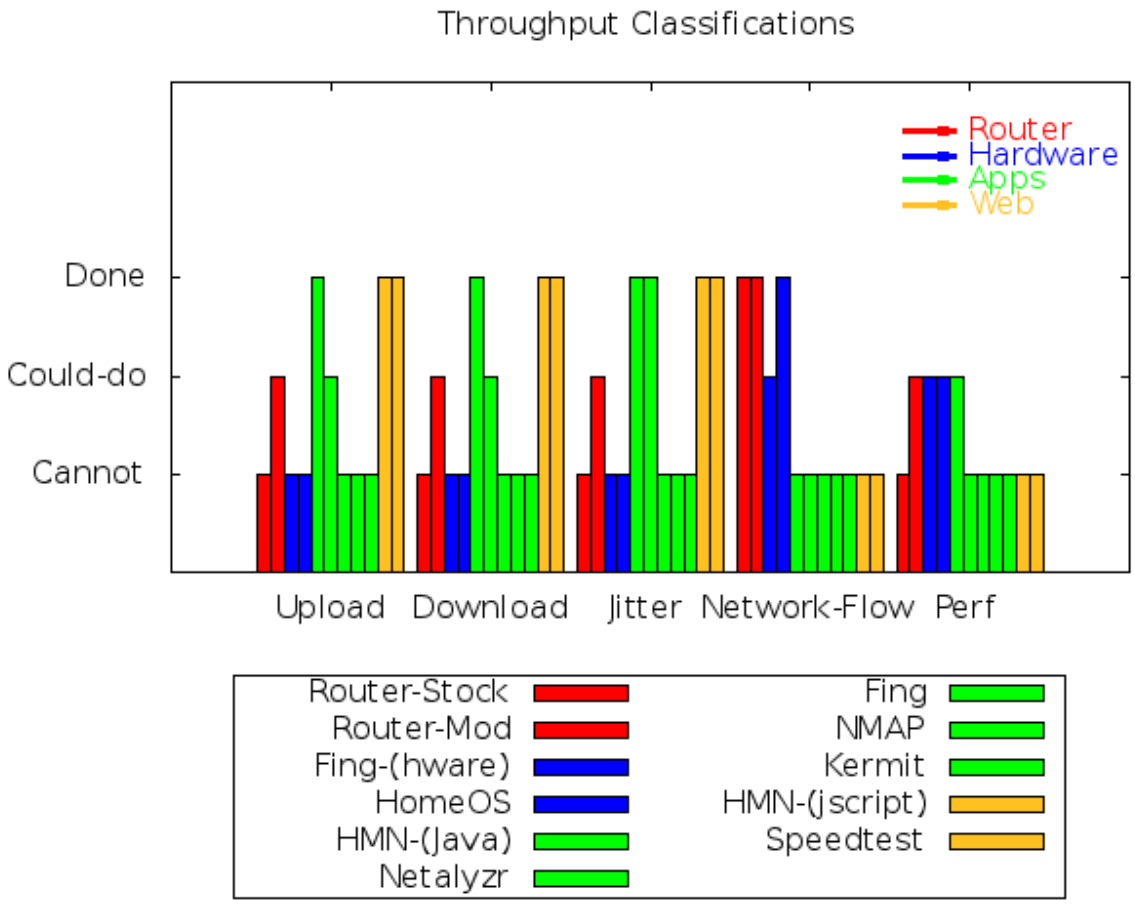

Figure 2: Throughput Classification

- Local device information: hardware, and software information for a given device. MAC address, name of host, networking information, and local software information (e.g. CPU, etc.).
- Remote Device information: fingerprint scan of network, including: TCP information, host and canonical names, and device types.
- Application list: locally running software list
- Network information: locally connected networks (e.g. Wifi, lans, etc.)
- Wireless information: available and browse-able networks

In addition, Figure 3, provides a view of data points that are available using each approach. While a stock router may have access to most of this information, it does not collect or store these data points. Apps collect these data points across the set of characteristics reviewed. Hardware approaches are similar to the Router approaches, and typically do not collect all of these characteristics. Web and scripting approaches do not have access to gathering most of this information as they run within a sandbox.

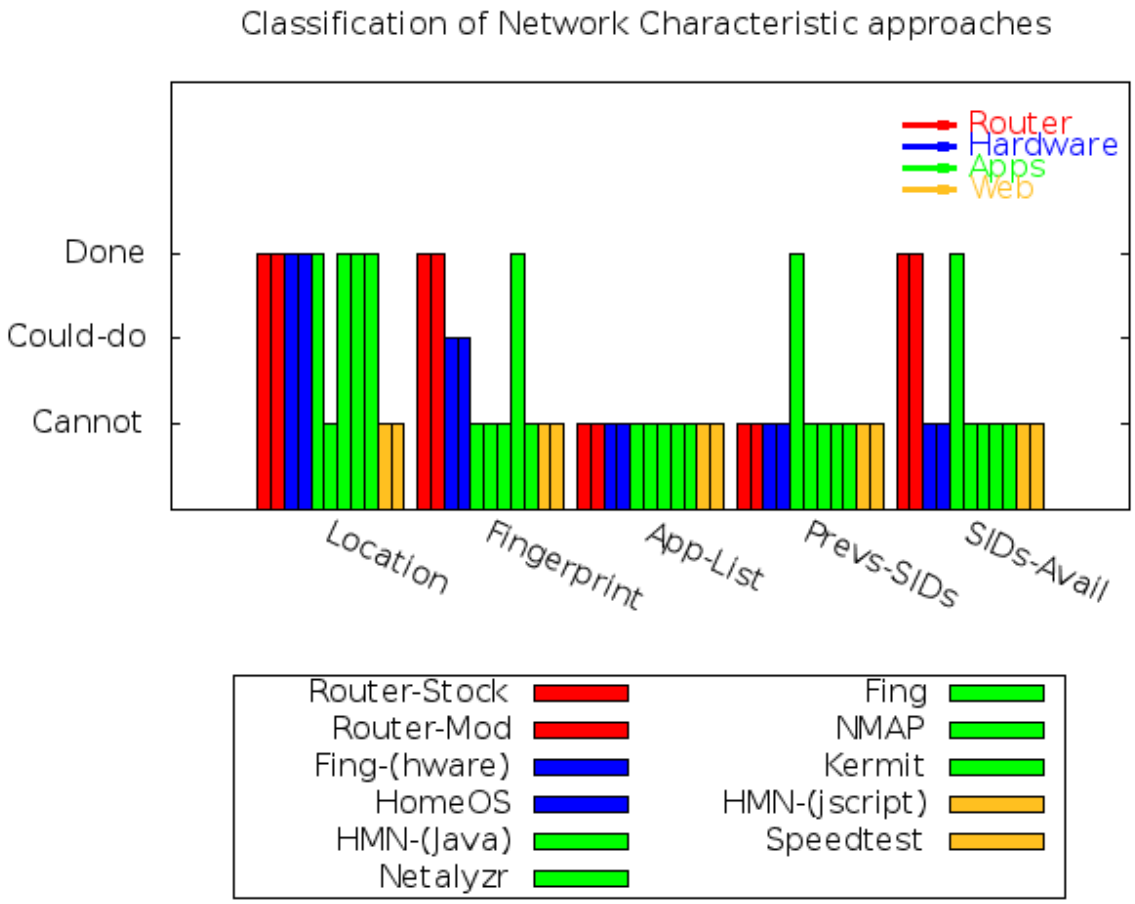

Figure 3: Network Characteristics Classification

5.3 Health

We move our area of focus toward health, and approaches used by the methods studied. Health includes local and remote networking, and Figure 4 shows health approaches by creating a classification of what can, and cannot be done in the following areas.

- DNS Health: this includes a health of the DNS infrastructure in-terms of networking, and reporting.
- Legacy Information: What devices previously attached to it.
- Security Review of Device
- Security Review of other Devices (via local connection)
- Recommendation System for Apps
- Health Check of device
- Network App profiling

5.4 Historical Norms

The classification of historical norms in data includes gathering point-in-time data, long-term availability of local data, global review of comparison data between local and other users experiences, legacy information using a longitudinal approach, and if the data is shareable to a wider community for research. We have created a classification of Norms in Figure 5, to help understand where there is overlap of methods in norms, and is a classification of what can, and cannot be done in the following items:

- Local Norms: Local information over time.
- Global Norms: Comparison of local and global scans.
- Legacy Information: What devices previously attached to it?
- Sharing of research data

6 Comparison of Approaches

We have created plots from the previous classifications to understand user participation associated with: impediment vs. incentive, sources vs. metrics, and local vs global data availability. These graphs provide a view into the measurement approaches and where there is similarity, and differences. The objective of these graphs are to help understand what types of information each approach provides (to users), along with incentives, impediments, as well as location and metrics. As an example, we look to understand the differences between what a Stock Router, modified Router, hardware approaches, App approaches, and Web approaches provides in-terms of information to the user. These graphs have data points that range between 1-4 (on both axis, starting at 1), which provide either easiest to hardest or low to high data information for the types plotted.

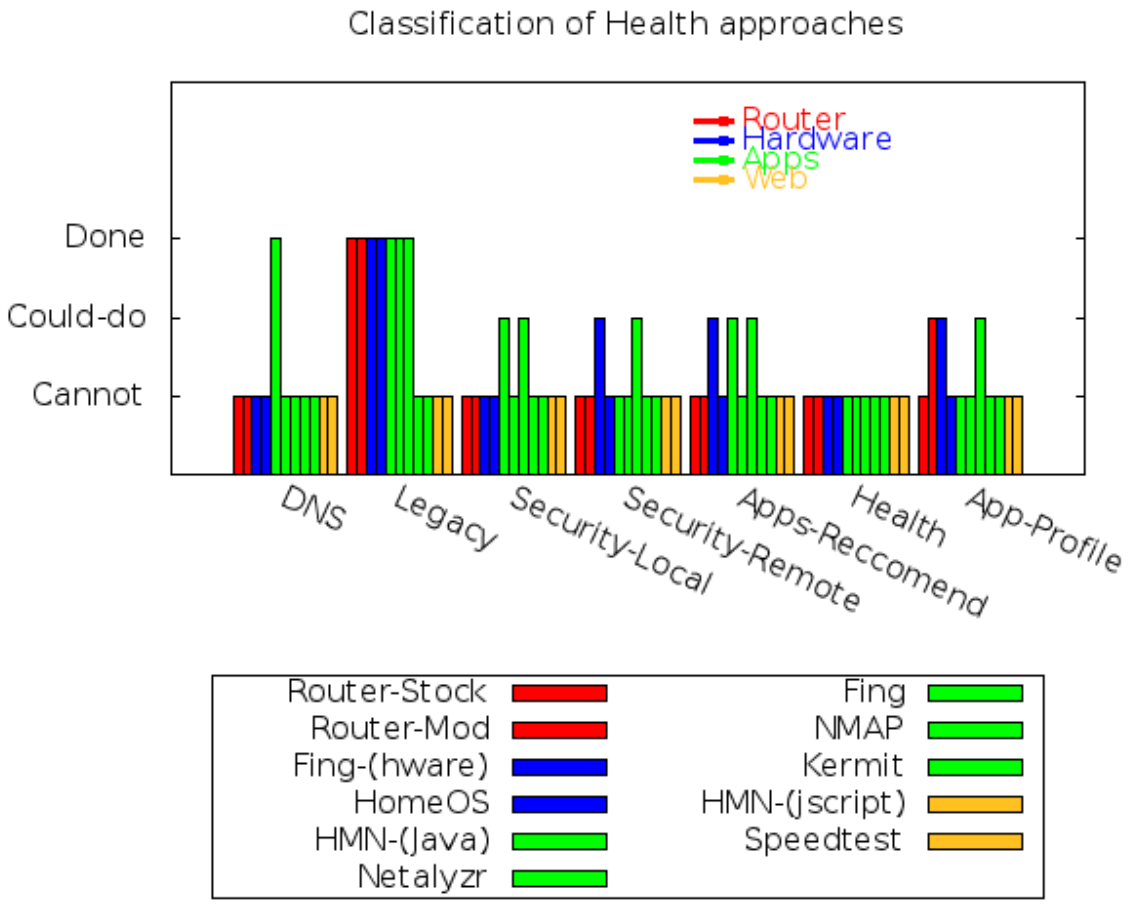

Figure 4: Health Classification

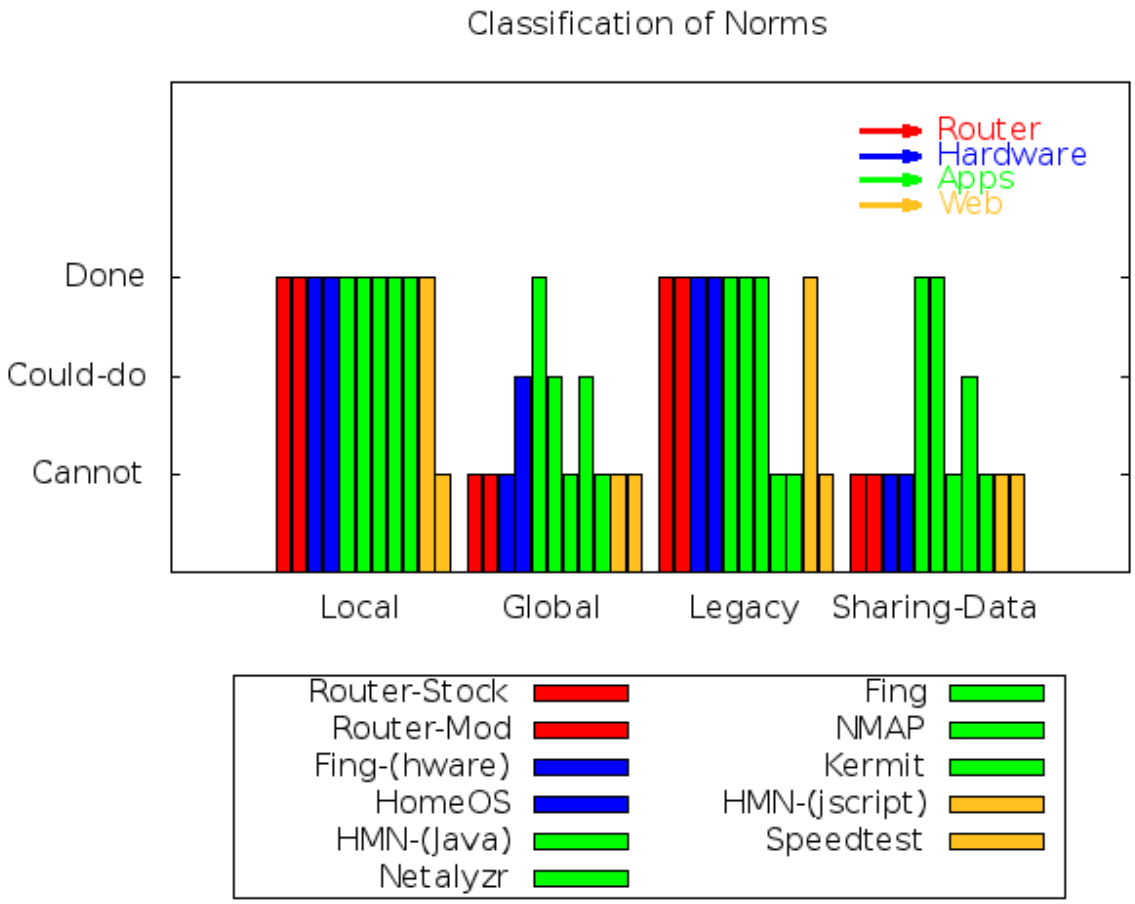

Figure 5: Historical Norms Classification

6.1 Incentives and Impediments

We have created an incentive vs. impediments Figure 6 to compare data of interest and tools, organized by approaches. Tools that reside in the upper left hand quadrant provide the most amount of data with the least amount of impediment. We can see that the cluster of tools reside in quadrants of the plot; As an example Web and Scripting have the least impediment, but provide the least amount of incentive (low).

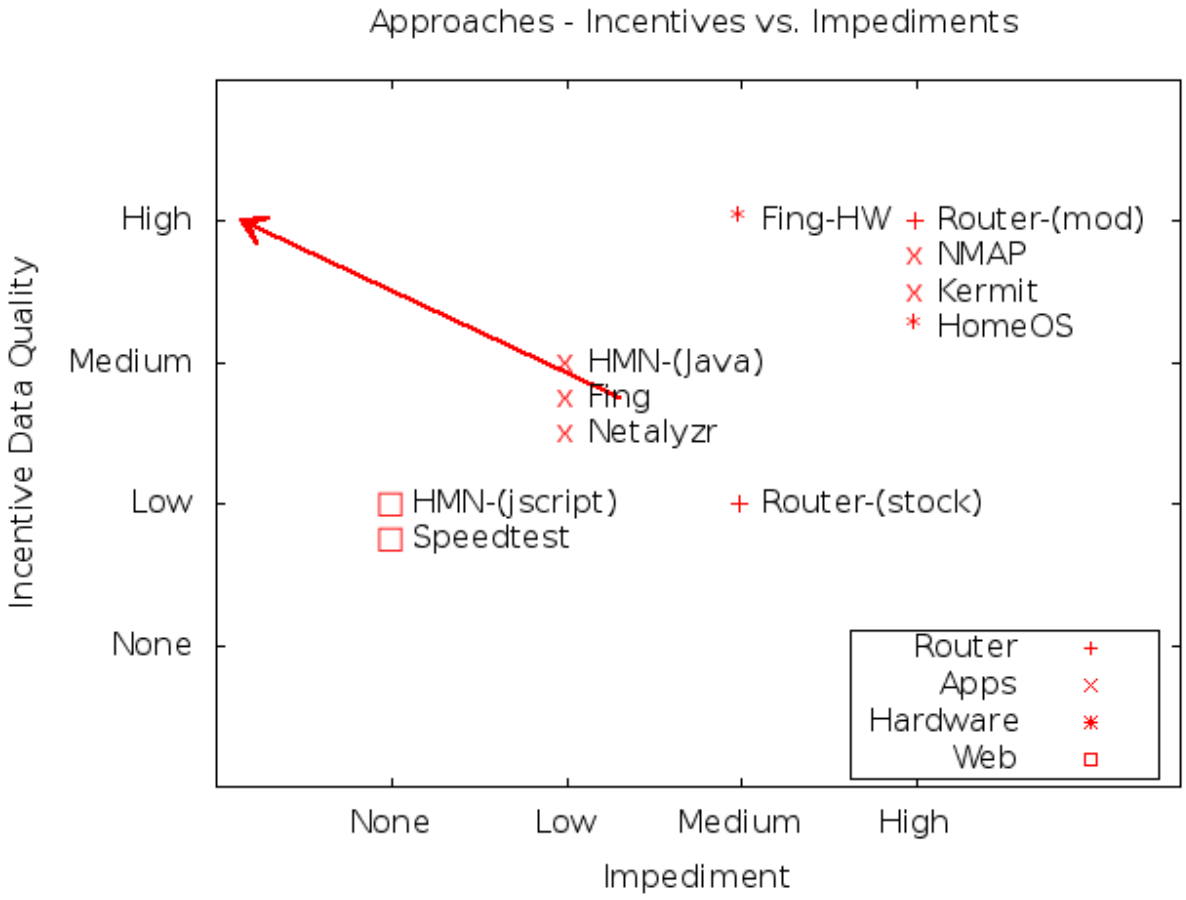

Figure 6: Incentive vs. impediments

6.2 Sources vs. Metrics

We have created a Sources vs Metrics scatter plot Figure 7, which compares sources vs data collections (or metrics) for each of the tools, organized by Approach. Figure 7 shows the flexibility of modification of sources, and configuration vs. the amount of quality data collected. The richest data and customization tools reside in the upper right hand quadrant. Tools such Nmap, and a modified-router provide the richest data sets, along with the most amount of customization

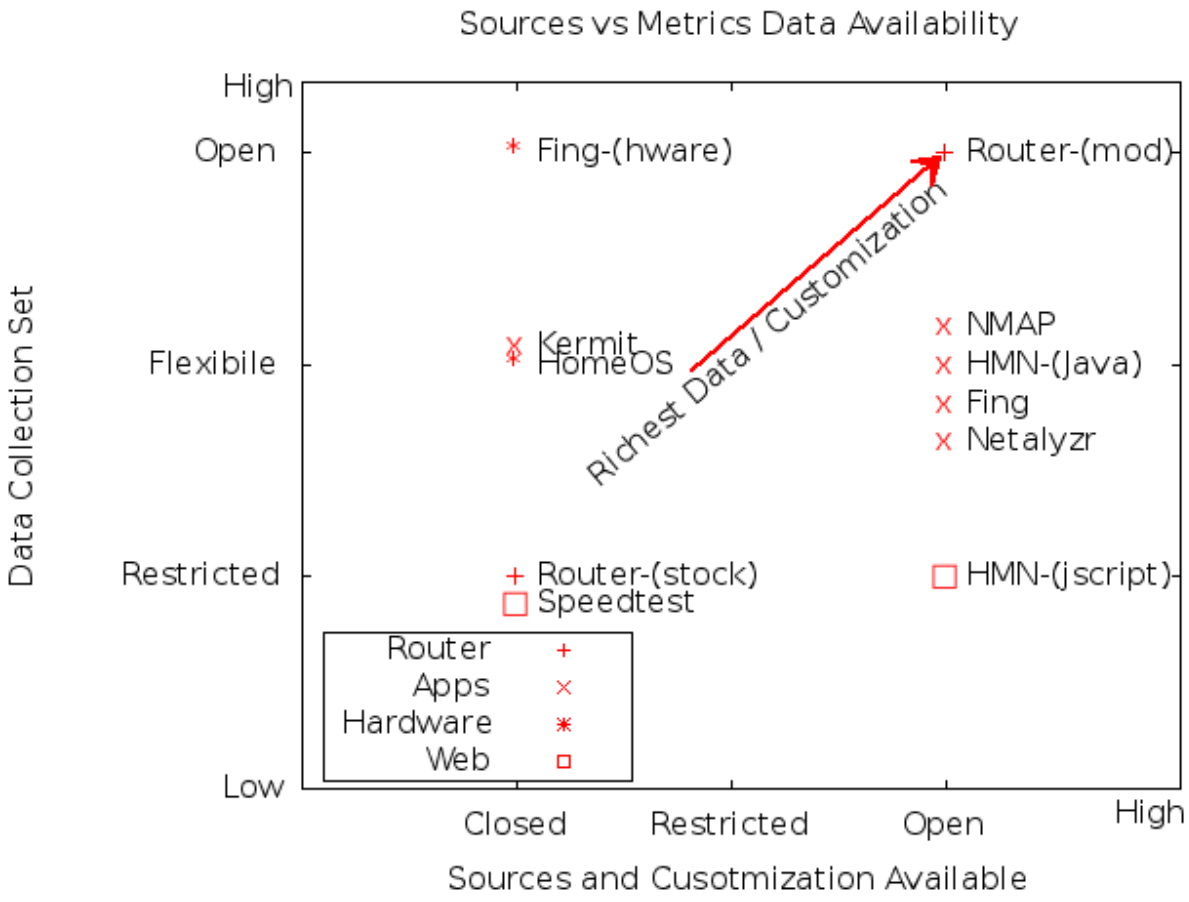

Figure 7: Sources vs. Metrics

6.3 Local vs. Global norms

We have created a Historical Norms, local vs global, plot of tools organized by Approaches. Figure 8 shows tools classified by information availability, and historical norms of data sharing The richest data and customization tools reside in the upper right hand quadrant. HMN-Java provides the richest norms as it provides both local and global norms to users and researchers, while there are no other tools that provide Global historical norms.

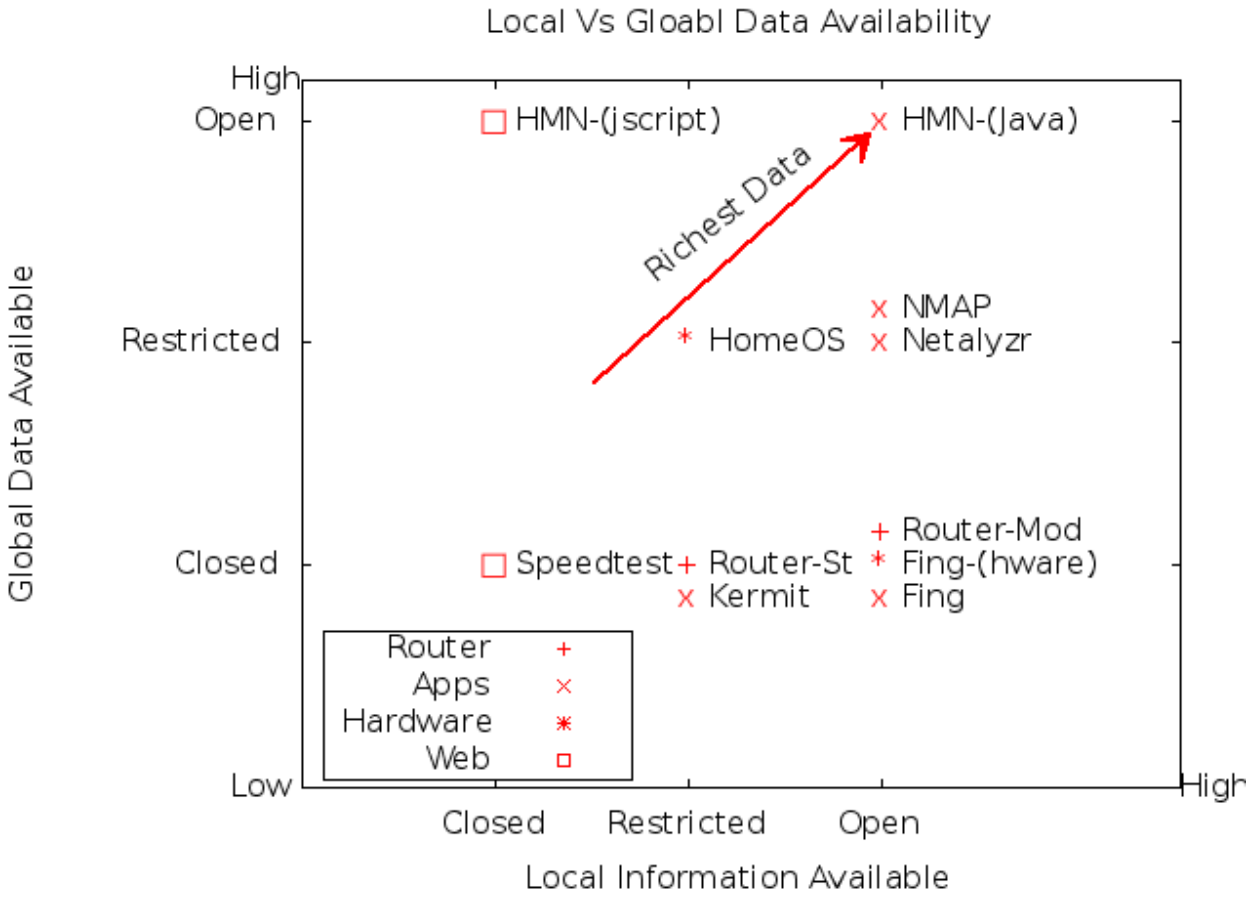

Figure 8: Historical Norms (Local Vs. Global)

7 Summary and Discussion of Collection Types

We next turn our attention to the tradeoff of these Approaches and data of interest, and provide a summary. We have reviewed four separate approaches to several data of interest and tools as part of HN access points: routers, Apps, hardware, and Web and scripting tools. While each of these collection approaches have merit, there are pros and cons of each of these approaches, which we detail.

The router and hardware approaches provide the highest level of information (as they are plugged directly into the network), and allow for the deepest dive into the network layer. These ap-

proaches have a single focus and do not provide users and researchers with a ubiquitous approach to network measurement. It also has the highest barrier to entry, and they do not scale to provide this local and global norm methodology. Hardware tools such as Fing (and other commercial and research tools) can provide single point of information, but do not collect the breadth of data provide global norms.

The Web and scripting collection types have minimal impediment to run as they execute either in a web browser or via a scripting environment that resides on the local system. The down side to this approach is that these collections can only provide a small percentage of results as compared to a router, hardware or Apps approaches, due to the sandbox they typically execute within.

Finally, the review of Apps approaches found that there is only a minimal impediment across the wide range of tools, as it can run on ubiquitously available mobile platform versus that of a fat client PC platform or a hard to configure hardware specific device. In addition, an App running in this space provides the most flexibility in-terms of incentive of information vs. the impediment of execution, and can also provide similar information of the hardware counterparts in most cases.

As a recap, the hardware approach is costly and can be complex to setup and configure, and thus has a high impediment to entry, but provides access as the incentive. An Apps research approach may be free to users, and require minimal impediment to install, configured, and execute and thus have a lower barrier to entry. A web/scripting approach may not provide enough information the user is looking to understand, but has the lowest barrier to entry as it executes within a web browser. To understand the data of interest provided from these approaches we have download tools, reviewed papers, and dichotomized the results and methods of the product/tool. These results found that Apps have the most flexibility in-terms of data of interest, as well as historical norms, and may provide the most optimal Approach, and thus tools, for users and researchers.

8 Future Work

In this section, we provide direction for future work and provide a discussion about How's My Network.

As we look to expand upon Apps work, we turn our focus to updating the HMN methodology, which can take advantage of the ubiquitous nature of mobile devices versus a high impediment of installing local hardware to run our network measurements. There are several Apps in the Android store that supply some of the information we are looking to gather, but these applications do not collate this into a study around configuration and local and global norms for users and researchers to review. These tools range in approaches and output, and look to provide basic information on hosts in a local network, and most of these tools are Ad driven or pay-for-Apps. Continuing the approaches used by HMN for HN discovery, this study looks to extend the data currently provided by adding the following information. As an example, the HMN mobile application determines host information using a variety of tools from the OS and native calls, such as netbios, smb, and DNS, which are also used by fing, and other commercial (non-research) tools.

- Historical Norms
  - Local norms of what is happening on the same network the App is running
  - Global norms of what is happening on similar or disjoint networks

- Minimal Impediment to entry
- Provides the right amount of Incentives to participate
- Digital Fingerprinting and Configuration of networks and Apps using Global and local Norms
- Using HCI approaches provide a unique way to display this information to end users with minimal impediments
  - E.g., the App is running and summarizes information about Local and Global norms for comparison.

Note: We are not aware of another study similar to this in the research space; there are Apps that collect some of this data, but are commercial and are pay for products, and thus does not provide this information.

A next phase discovery of HN would also include approaches of active and passive scanning techniques. The novel approach of gathering data to understand the configuration between hardware and Apps would allow us to use services for Android, without jail-breaking the phone, to capture the needed summary for local and global norms and analysis. This passive approach should allow us to determine well-known systems and allow for a fingerprinting technique of discovered devices.

We conjecture that users are more apt to run an App approach, such as HMN, that has minimal impediments to execution and provides local and global norms. The advantages of the HMN is that it can be run on a wide range of Android mobile devices, and requires only minimal impediment to the user for downloading; the convenience of a ubiquitous platform vs. that of a customized set of tools on a router (e.g. DD-WRT) or on a customized PC for the execution of a fat client, which requires an install presence on their local system, or that of a browser based tool.

8.1 How's My Network

How's My Network (HMN) is an open approach to HN study, as previously mentioned. The HMN work done in [68] used some of the techniques reviewed to detect domain connections, devices, and configurations. We look to build on this collection method, so that we can determine Apps running/available on a Mobile device (locally), similar to [37]. As an example, when running the HMN Mobile app (e.g. from Androdid-5dc) we may produce output that includes status (present, not available), Device type (canonical Name of Device), and Apps running on the host device. The HMN tool also looks to understand throughput (Up/Down), DNS Health, Application configuration, Wifi access list, Jitter, device health, and legacy information in and around these items for local and global norms. The difference between the HMN Mobile tool and commercial or research tools, is that we are also looking to understand local and global norms as part of the study; and we look to share this information for future research.

In this previous work, we compiled a database of Hardware Devices along with all of the corresponding manufacturer identifiers (MAC), which has not previously existed. This list includes the following information: MAC Address, Date of certification, Manufacturer/Brand, Product, Model number, Category (Phones, Computer Accessories, Other), Hardware Version, Firmware

Version, OS Version (if available), and frequency info (telephony and Wifi). We have overlapped corresponding DB types into one grouping, so that all types from one manufacturer are part of a super-set. As an example, a subset of the LG Electronics (Phones) contains the following properties. With this information, we have the ability to understand global manufacturer MAC addresses associated with Model #s and current versions of the software running on the given devices. A classification of this information can be seen in Table 5, which provides information around device activity (status), device type, and applications available on this device.

Table 5: Device List

Device List		
Status	**Device**	**App**
Present	ChromeCast	NA
Not Avilable	Sling	NA
Present	Android-5dc	VLC
Present	Android-5dc	ConnectBot
Present	Android-5dc	Spotify
Present	Android-5dc	...
Present	Android-5dc	Outlook
Present	Android-5dc	NFL Mobile
Present	Android-5dc	2048 Puzzle
Present	Android-5dc	Gmail

We look to understand basic information around the network where the device resides, including: how to gather a database of Devices (Wifi) and match them to manufacturer? To help answer this questions we have collected a series of data sets of devices and matching information into a database of devices as part of discovery. In this previous study we created a database (via shell, and scripting languages) to collect this information and update the App on the fly or via a stored DB. We have also include the tools to determine upload/download speed, jitter, Wifi network usage, App detection, and general health overview, which are all part of the study. We have compiled a database of Hardware Devices along with all of the corresponding manufacturer identifiers (MAC), which to our knowledge has not previously existed. We looked at how to match this database of Devices (Wifi) to manufacturer using the following methodology.

As next steps we look to extend the HMN work to understand the configuration challenges networks have by extending the work around classification and norms to include the discovery of configuration of these domains that are both accurate, and useful, and includes information around the HN, and we look to further classify these into the following subcategories to help understand device characteristics, platforms they execute within, components of tools these fall into, and the types of services they provide. We propose a review into the following expanded data of interest set to review:

- **Device Characteristics**: PC and Mobile devices and similar hardware, as well devices such as: Wifi, IoT, and similar.

- **Platforms**: The type of environment these tools run within, such as Android App or an executable.
- **Components**: Security, Privacy, and Health, and how the tools fall into each of these areas.
- **Services**: Types of Apps running on the local device: e.g. SMS, Phone, encryption, proxy, application, networking, virus/phishing, safe browsing, Email, Battery, IOT, etc.

References

[1] Alibba. *Alibaba Mobile Security*. https://play.google.com/store/apps/details?id=com.eset.ems2.gp&hl=en. [] 2015-12-07.

[2] Frank Andrus. "Beyond scan and block: an adaptive approach to network access control". In: *Network Security* 2011.11 (2011), pp. 5–9.

[3] *Application and Software*. https://www.techopedia.com/definition/4224/application-software. Accessed: 2018-03-17.

[4] Abdullahi Arabo, Ian Brown, and Fadi El-Moussa. "Privacy in the age of mobility and smart devices in smart homes". In: *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*. IEEE. 2012, pp. 819–826.

[5] Andrés Arcia-Moret et al. "Intelligent network discovery for next generation community wireless networks". In: *Wireless On-demand Network Systems and Services (WONS), 2016 12th Annual Conference on*. IEEE. 2016, pp. 1–7.

[6] BullGuard. *BullGuard Mobile Security*. https://play.google.com/store/apps/details?id=com.bullguard.mobile.mobilesecurity&hl=en. [] 2015-12-07.

[7] Kenneth L Calvert et al. "Instrumenting home networks". In: *ACM SIGCOMM Computer Communication Review* 41.1 (2011), pp. 84–89.

[8] Daniel Camps-Mur et al. "Enabling always on service discovery: Wifi neighbor awareness networking". In: *IEEE Wireless Communications* 22.2 (2015), pp. 118–125.

[9] Jacob Carlsson. *Comparison in functionality between a closed and two open source distributions in a router*. 2016.

[10] Ranveer Chandra, Christof Fetzer, and Karin Hogstedt. *Adaptive topology discovery in communication networks*. US Patent 7,366,113. Apr. 2008.

[11] *Cheetah Mobile Clean Master*. http://www.cmcm.com/en-us/clean-master/. Accessed: 2018-03-17.

[12] Marshini Chetty and Nick Feamster. "Refactoring network infrastructure to improve manageability: a case study of home networking". In: *ACM SIGCOMM Computer Communication Review* 42.3 (2012), pp. 54–61.

[13] Marshini Chetty et al. "Why is my internet slow?: making network speeds visible". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2011, pp. 1889–1898.

[14] Luca Chittaro. "Visualizing information on mobile devices". In: *Computer* 39.3 (2006), pp. 40–45.

[15] *Cisco Discovery Protocol*. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html. Accessed: 2018-03-17.

[16] Crypt4All. *Sophos Mobile Security*. https://play.google.com/store/apps/details?id=com.codewell4.Crypt4AllLite&hl=en. [] 2015-12-07.

[17] Anita D'Amico et al. "Integrating physical and cyber security resources to detect wireless threats to critical infrastructure". In: *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*. IEEE. 2011, pp. 494–500.

[18] *DD-WRT*. https://www.dd-wrt.com/site/index. Accessed: 2018-01-05.

[19] Lucas DiCioccio, Renata Teixeira, and Catherine Rosenberg. "Measuring home networks with homenet profiler". In: *International Conference on Passive and Active Network Measurement*. Springer. 2013, pp. 176–186.

[20] Colin Dixon et al. "An operating system for the home". In: *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation*. USENIX Association. 2012, pp. 25–25.

[21] Colin Dixon et al. "The home needs an operating system (and an app store)". In: *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*. ACM. 2010, p. 18.

[22] *Dojo hardware security and privacy device*. https://dojo.bullguard.com/. [] 2008-03-17.

[23] Jack Poller Doug Cahill. *An Adaptive and Layered Approach to Endpoint Security*. https://www.bitdefender.co.th/media/wysiwyg/gravityzone/elite-security/ESG-White-Paper-Bitdefender-Jun-2017.pdf. [DYN Networks]. 2017-16-01.

[24] Jack Poller Doug Cahill. *An Adaptive and Layered Approach to Endpoint Security, June 2017, ESG White Paper*. https://www.bitdefender.co.th/media/wysiwyg/gravityzone/elite-security/ESG-White-Paper-Bitdefender-Jun-2017.pdf. [] 2008-03-17.

[25] Jack Poller Doug Cahill. *Cujo hardware security monitoring device*. www.getcujo.com. [] 2008-03-17.

[26] DYN. *Measuring DNS Performance with Open Recursive Name Servers*. https://dyn.com/blog/dns-performance/. [DYN Networks]. 2015-12-07.

[27] W Keith Edwards et al. "Advancing the state of home networking". In: *Communications of the ACM* 54.6 (2011), pp. 62–71.

[28] *Fing-Network Tools*. https://www.fing.io/. Accessed: 2018-03-17.

[29] Marcel Flores, Alexander Wenzel, and Aleksandar Kuzmanovic. "Oak: User-Targeted Web Performance". In: *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE. 2017, pp. 2654–2655.

[30] *Flying Squirrel is the Department of Defense standard wireless discovery and mapping application. It runs on Windows and Linux using commercial laptops, wireless cards, and GPS devices.* https://www.nrl.navy.mil/itd/chacs/5545/flying-squirrel/FAQ. Accessed: 2018-03-17.

[31] Rebecca E Grinter et al. “The ins and outs of home networking: The case for useful and usable domestic networking”. In: *ACM Transactions on Computer-Human Interaction (TOCHI)* 16.2 (2009), p. 8.

[32] Rebecca E Grinter et al. “The work to make a home network work”. In: *ECSCW 2005*. Springer. 2005, pp. 469–488.

[33] Lucas Guardalben et al. “A cooperative hide and seek discovery over in network management”. In: *Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP*. IEEE. 2010, pp. 217–224.

[34] Michael Hall and Raj Jain. “Performance analysis of openvpn on a consumer grade router”. In: *cse. wustl. edu* (2008).

[35] Hadrien Hours et al. “A study of the impact of DNS resolvers on CDN performance using a causal approach”. In: *Computer Networks* 109 (2016), pp. 200–210.

[36] *Internet Speed Meter Lite*. `https://play.google.com/store/apps/details?id=com.internet.speed.meter.lite&hl=en`. [] 2008-03-17.

[37] Yunhan Jack Jia et al. “Open Doors for Bob and Mallory: Open Port Usage in Android Apps and Security Implications”. In: *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on*. IEEE. 2017, pp. 190–203.

[38] Jaeyeon Jung et al. “DNS performance and the effectiveness of caching”. In: *IEEE/ACM Transactions on networking* 10.5 (2002), pp. 589–603.

[39] Murad Kaplan et al. “How’s My Network? Predicting performance from within a Web browser sandbox”. In: *Local Computer Networks (LCN), 2012 IEEE 37th Conference on*. IEEE. 2012, pp. 521–528.

[40] Zolidah Kasiran and Juliza Mohamad. “Throughput performance analysis of the wormhole and sybil attack in AODV”. In: *Digital Information and Communication Technology and it’s Applications (DICTAP), 2014 Fourth International Conference on*. IEEE. 2014, pp. 81–84.

[41] *Kaspersky Lab Internet Security*. `https://usa.kaspersky.com/internet-security`. Accessed: 2018-03-17.

[42] *Keezel hardware security and privacy device*. `https://keezel.co/`. [] 2008-03-17.

[43] Athar Ali Khan, Mubashir Husain Rehmani, and Yasir Saleem. “Neighbor discovery in traditional wireless networks and cognitive radio networks: Basics, taxonomy, challenges and future research directions”. In: *Journal of Network and Computer Applications* 52 (2015), pp. 173–190.

[44] Hyojoon Kim and Nick Feamster. “Improving network management with software defined networking”. In: *IEEE Communications Magazine* 51.2 (2013), pp. 114–119.

[45] *Kismet Wireless Scanner*. `https://www.kismetwireless.net/android-pcap/`. Accessed: 2018-03-17.

[46] Jan Willem Kleinrouweler. “Enhancing over-the-top video streaming quality with DASH assisting network elements”. In: *Adjunct Publication of the 2017 ACM International Conference on Interactive Experiences for TV and Online Video*. ACM. 2017, pp. 113–116.

[47] Jan Willem Kleinrouweler, Britta Meixner, and Pablo Cesar. “Improving Video Quality in Crowded Networks Using a DANE”. In: *Proceedings of the 27th Workshop on Network and Operating Systems Support for Digital Audio and Video*. ACM. 2017, pp. 73–78.

[48] Christian Kreibich et al. “Netalyzr: illuminating the edge network”. In: *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*. ACM. 2010, pp. 246–259.

[49] *LastPass*. https://lastpass.com/. Accessed: 2018-03-17.

[50] *LEEDE project, 2014*. https://www.bufferbloat.net/projects/cerowrt/wiki/. Accessed: 2018-03-17.

[51] Yadong Li et al. “Research based on osi model”. In: *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*. IEEE. 2011, pp. 554–557.

[52] *Meshlium IoT Gateway Hardware*. http://www.libelium.com/products/meshlium/. Accessed: 2018-03-17.

[53] *Mtoolbox web port scanner*. mxtoolbox.com. [] 2008-03-17.

[54] *Net Mapper*. https://play.google.com/store/apps/details?id=com.wwnd.netmapper&h. Accessed: 2018-03-17.

[55] *NetMapper App.* https://play.google.com/store/apps/details?id=com.wwnd.netmapper&h. Accessed: 2018-03-17.

[56] *NMAP*. https://nmap.org/. Accessed: 2018-03-17.

[57] *Norton Mobile Security 3.15*. http://norton.com. Accessed: 2018-03-17.

[58] Mihai Novitchi. *Anti-malware emulation systems and methods*. US Patent 8,407,797. Mar. 2013.

[59] Ookla. *OoklaSpeedtest*. https://play.google.com/store/apps/details?id=org.zwanoo.android.speedtest&hl=en. [] 2014-12-07.

[60] Orbot. *Orbot Proxy*. https://play.google.com/store/apps/details?id=org.torproject.android&hl=en. [] 2014-12-07.

[61] *PCAP for Android*. https://play.google.com/store/apps/details?id=jp.co.taosoftware.android.packetcapture. Accessed: 2018-03-17.

[62] *PEW Home Networking Review 2017*. http://www.pewinternet.org/fact-sheet/internet-broadband/. Accessed: 2018-01-05.

[63] Erika Shehan Poole et al. “Computer help at home: methods and motivations for informal technical support”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2009, pp. 739–748.

[64] Erika Shehan Poole et al. “More than meets the eye: transforming the user experience of home network management”. In: *Proceedings of the 7th ACM conference on Designing interactive systems*. ACM. 2008, pp. 455–464.

[65] R Kelly Rainer et al. *Introduction to information systems*. John Wiley & Sons, 2013.

[66] Dave Randall. “Living inside a smart home: A case study”. In: *Inside the smart home*. Springer, 2003, pp. 227–246.

[67] *RaTTrap hardware security and privacy device*. www.myrattrap.com. [] 2008-03-17.

[68] Alan Ritacco, Craig Wills, and Mark Claypool. "How's My Network? A Java Approach to Home Network Measurement". In: *Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th Internatonal Conference on*. IEEE. 2009, pp. 1–7.

[69] *Router Interrogation. Colby Lahaie, David Paradise. Research Project work done as part of the Senator Patrick Leahy Center for Digital Investigation, Champlain College, 2013*. https://www.champlain.edu/Documents/LCDI/archive/POST_ME_Router-Interrogation-ReportPDF.pdf&usg=AOvVaw2tHbiS9vxwV3saq2tvq7Qa. Accessed: 2018-03-17.

[70] *Security and Apps on Android*. http://resources.infosecinstitute.com/security-hacking-apps-android/. Accessed: 2018-01-05.

[71] *Security and Apps on Android*. http://resources.infosecinstitute.com/security-hacking-apps-android/. Accessed: 2018-03-17.

[72] Erika Shehan and W Keith Edwards. "Home networking and HCI: What hath God wrought?" In: *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM. 2007, pp. 547–556.

[73] Ramesh K Sitaraman. "Network performance: Does it really matter to users and by how much?" In: *Communication Systems and Networks (COMSNETS), 2013 Fifth International Conference on*. IEEE. 2013, pp. 1–10.

[74] Sophos. *Sophos Mobile Security*. https://play.google.com/store/apps/details?id=com.sophos.smsec&hl=en. [] 2015-12-07.

[75] *Spiceworks Scanner*. community.spiceworks.com/tools/port-scan?blog_2484. [] 2008-03-17.

[76] Hengky Susanto. "Congestion control with QoS through network utility maximization". PhD thesis. University of Massachusetts Lowell, 2014.

[77] Hengky Susanto, Byung Guk Kim, and Benyuan Liu. "User Tolerance and Self-Regulation in Congestion Control". In: *arXiv preprint arXiv:1706.03632* (2017).

[78] Andrea Tagarelli and Roberto Interdonato. "Who's out there?: identifying and ranking lurkers in social networks". In: *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. ACM. 2013, pp. 215–222.

[79] *TCP and UDP Nmap port scanning web tool*. pentest-tools.com. [] 2008-03-17.

[80] TextSecure. *TextSecure Private Messenger*. http://download.cnet.com/TextSecure-Private-Messenger/3000-2150_4-76145455.html. [] 2014-12-07.

[81] *Understanding Mobile Apps*. https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps. Accessed: 2018-03-17.

[82] Mark Unwin. *Open-AudIT*. http://www.opmantek.c. [] 2008-03-17.

[83] Bjørn J Villa. "Enhancing Quality Aspects of Adaptive Video Streamingin Home Networks". In: (2014).

[84] *Wifi Analyzer*. https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer&hl=en. Accessed: 2018-03-17.

[85] *Wifi Analyzer App*. https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer&hl=en. Accessed: 2018-03-17.

[86] *WiFi Connection Manager*. https://play.google.com/store/apps/details?id=com.roamingsoft.manager&hl=en. Accessed: 2018-03-17.

[87] *WiFi Connection Manager*. https://play.google.com/store/apps/details?id=com.roamingsoft.manager&hl. Accessed: 2018-03-17.

[88] *WiFi-Master-Speed-Test-Booster*. https://play.google.com/store/apps/details?id=com.leo.wifi&hl=en. Accessed: 2018-03-17.

[89] *Windows Speedtest*. http://www.speedtest.net/apps/windows. Accessed: 2018-03-17.

[90] Yiannis Yiakoumis et al. "Slicing home networks". In: *Proceedings of the 2nd ACM SIGCOMM workshop on Home networks*. ACM. 2011, pp. 1–6.

[91] Shuai Zhao et al. "Study of user QoE improvement for dynamic adaptive streaming over HTTP (MPEG-DASH)". In: *Computing, Networking and Communications (ICNC), 2017 International Conference on*. IEEE. 2017, pp. 566–570.

[92] Xuzi Zhou. *Understanding home networks with lightweight privacy-preserving passive measurement*. University of Kentucky, 2016.