ISSN 2047-3338

Restructuring Network Infrastructure with Software Defined Networking

Muhammad Rizwan[1] Ahmad and M. J. Qureshi[2]

[1,2]Department of Computer Science and Engineering, UET, Lahore, Pakistan

[1]welcomengineer@hotmail.com, [2]mjunaiduet@gmail.com

Abstract– **Home network is very challenging to manage because of the complexity of underlying infrastructure. Network's underlying complexity is either hidden or exposed by the existing network interfaces, but the visible information is not necessarily helpful for the user to complete the desired tasks. However, underlying network and protocols can be redesigned as a result of advances in software defined networking. As a result of these advances, the designers can move the complexity of the network infrastructure from the user and can also eliminate it entirely. This paper focuses on what can be made visible to the user in the modern home network infrastructure design, performance and some of the policies. We also examine whether changing the underlying network infrastructure without affecting the previous functionality should cause us to refine these choices.**

Index Terms– **Home Networking, Network Management, Network Monitoring and SDN**

I. INTRODUCTION

HOME users always like to have a functional network connection to get benefits from the usage of various complicated applications and various services. But experts found it very difficult to manage and secure home networks because of the complexity of systems. It is also very difficult to troubleshoot the home network [31], [21].

A home network must provide support for various types of devices, applications and users, and protocols for providing such support are also very complex, so the complexity in home networks is inherent. A lot of challenges are involved in changing the network infrastructure [34]. Because of these challenges and the network complexity, the interface designers for the home network are forced to either hide or expose some of the network function so that users can achieve their required goals (e.g., IP should be exposed when configuring default functionality or setting up router so that complexity remains hidden) [24].

Unfortunately, challenges and difficulties involved in restructuring the network infrastructure have put constraints on network interface designers. In this paper, it is shown that network interface improvements can be obtained only when designers and network architects work together to put their efforts in co-designing of the underlying infrastructure and infrastructure controlling interfaces. It is suggested by the researchers that restructuring of the network infrastructure can improve interfaces for the home networks without affecting the existing functionality [32]. Now, with the help of recent developments in SDN, it is possible to restructure underlying network infrastructure without complete overhauling of the internet [17], [14].

In this paper, we will explore in detail the opportunities for restructuring the home network infrastructure to improve the system visibility. We will also suggest how to improve user experience by restructuring the network functions. We highlight three things. First, where infrastructure, performance and policies of existing home networking are either too hidden or too visible from end-users and how this affects the user's experiences.

Second, we argue that current home networking infrastructure constraints does not limit the designers. The designers and the network researchers can work together in network functions restructuring so that interfaces can be created to better accommodate the user.

Third, examples are provided of how network function's restructuring can provide intentional user interfaces.

II. INFRASTRUCTURE AND VISIBILITY

First, we explore previous work that presents in detail the major role of functionality visibility in the network infrastructure design and will provide two conditions that must be true about the network infrastructure so that the interface can expose it. After this, we present previous work describing the role of functionality visibility in the home networking infrastructure and interfaces design. Finally, we describe some details on SDN (Software Defined Networking).

A) Network Infrastructure Visibility

Infrastructure represents the building blocks and frameworks to support the user's everyday activities [7]; e.g. it may be roads, software systems, electricity grids. Until infrastructure breaks, it remains unnoticed [33], [6]. In home networking infrastructure, the networking complexity of the systems that support internet connectivity sharing, is exposed during fault occurrence. This is an open issue to design the network interfaces that provide the facility to home user's to fix problems and troubleshoot networks without being exposed to the underlying mechanics and networking infrastructure. In fact, the home users want a fully functional network, so it is reasonable to inquire whether they need anything that should be made visible.

We argue that some aspects of the complicated systems always need human intervention, so network infrastructure cannot be totally invisible. For example, without giving some input, the home network cannot be able to execute a user's intent intelligently. It is agreed that network infrastructure should support the user's tasks; we believe that information, helping a user to understand the system's functionality, is very important to allow users to implement various functions and network policies. In this paper, we provide an overview of how to improve what functionality is visible and invisible.

Belotti and Edwards [35] suggest that in order to improve the system's intelligibility and user understanding about the system's various actions, it is advisable to provide the visibility into system's internals. Similarly, in order to improve users' understanding of a system, the system should expose some metaphors that represent how the system is working [25]. For example, dropped connection between two systems may cause a file transfer failure, but the progress bar does not show the cause of failure.

When infrastructure should be made visible?

In this paper, we will focus on the following design question: When and how much information should be made visible about the network infrastructure to facilitate a user in better understanding of a system and get the end-goals; and how this type of visibility can be supported by the network infrastructure?

In case of home networking, the visibility of network infrastructure should be based on the following:

1) If it helps in the improvement of situational awareness.

2) If it provides some actionable information.

Improvement in the situational awareness refers to the information by which user can get more awareness about the system environment and help the users in decision making for their goals.

Actionable information means the information about which a user can do something.

For example, in the home network, the information which helps to indicate the presence of an unauthorized device helps in the improvement of situational awareness and is actionable, i.e. the user can take appropriate steps to block the access of the device to the network.

The web page that provides the IP address assignment information or hardware addresses of other devices does not satisfy these criteria. Ideally the network infrastructure part that neither provide any help in the improvement of situational awareness nor present any actionable information will disappear from daily use [4].

B) *Visibility in Home Networking*

The details about the network infrastructure and protocols, exposed by interfaces currently used for home networking, are generally complex and irrelevant e.g. SSID and MAC. The Information that helps in the improvement of situational awareness is not visible to end-users. Same is the case with actionable information. It is possible that a home user can exhaust bandwidth cap on internet services without any realization that they have done it [31].

The previous work has focused on the difficulties faced by the existing home network users [5], [16], [18], [19]. Many of these difficulties are rooted in the network design infrastructure which was not created for home users [34]. We believe that restructuring the network infrastructure and redesigning of interfaces is a big challenge due to the seriousness of usability problems.

In order to address difficulties in home networking, some approaches have been proposed by researchers. Along with other approaches, it includes the following two approaches as well:

1) Bandage approach: this approach helps in designing of interfaces to mask network complexity.

2) Clean Slate approach: it helps in the complete overhaul of internet protocols so that the protocols can be more user-centric [8].

It is not tenable to redesign the network from scratch, so most of the time, bandage model is applied by the designers e.g., Eden System helps to configure network by direct manipulation interfaces [3].

Edwards et al. introduced a notation of constrained possibilities [23]. It suggested that it is possible to constrain the uses and interfaces of infrastructure at first place with its design. It is also suggested that changes in the underlying infrastructure are required when altering these constraints. We argue that it is possible to overcome the constrained possibilities by software defined networking (SDN) for home network interfaces. "Co-design" approach is possible by restructuring the underlying network, restructuring the underlying network makes a "co-design" approach possible, whereby the interface and infrastructure design take each other and user into account, as with user centered design approach.

C) *Software Defined Networking: Enabling Restructuring*

Software defined networking (SDN) is a latest trend in network infrastructure design and protocols, high level software programs control the behavior of network protocols and devices, rather than the hardware [17]. The intelligence of the network is refactored by SDN so that network behavior definition logic resides in a logically centralized software controller. The controller issues the commands to the network devices such as switches, routers and other devices. These commands define the behavior of these devices.

The controller may be centralized logically or physically and it may be separate from the traffic controlling devices. This separation refers to the placement of control in software elements residing on same device. For example, software control in home networking may reside on router at home or in cloud outside of home [2]. Radical restructuring of the network infrastructure is enabled by SDN in a specific case of home network. The high level software programs can control the behavior of previously used home network devices such as access points and routers. As a result of this, network functions such as decision making protocols of when and how to forward traffic, how to measure performance and many more, can be refactored.

The goal of network restructuring is to support intelligibility and control [26]. Unlike the reflective representation of an interactive system about its own activity, SDN provides new features of network control and monitoring. We argue that it is easier to expose a certain level of complexity by network function refactoring, and this refactoring helps to design interfaces to expose information that can improve situational awareness and an end user can take action about.

Following this section, we highlight the previous work that shows where current home network infrastructure is either too hidden or too visible to end-user. After this, we explain how network refactoring can make it possible for co-designed network interfaces for users. Network performance, policies and infrastructure are also examined.

III. HOME NETWORK INFRASTRUCTURE

Home network infrastructure consists of the following:

1) Networking devices such as routers and access points.

2) Interconnecting devices such as laptops, mobile phones and desktops.

3) Technologies for interconnection of devices such as cables.

A) Setting up the Network

Visibility in Installation: Users are required to manipulate low level network protocols in the installation and configuration of home network, e.g., when a home user installs a router for the first time, the differences between the wired connections to internet or WAN and wired connections in their home or LAN must be known to them. Many users did not consider these distinctions and configure the routers incorrectly [10].

After a home user succeeds in router configuration to internet, he must fight to understand the confusing technical terminology such as Dynamic Host Configuration Protocol configuration, wireless channel encryption and IP addressing for connecting devices with internet. Because of these technicalities, users simply prefer to configure router with default settings. Because of complexity in establishing basic network connectivity, the designing of a usable interface for home networking setup is incredibly difficult. Some existing systems such as NetPrints [37] and Network Magic [12] use wizards for setup and configuration become easier by physical interfaces or auto configuration of devices, to hide complexity from users.

Reduce visibility by refactoring basic connectivity: We can make the network interfaces; we design, less constrained by restructuring underlying network infrastructure. It is possible to move some complexity into the router by restructuring the underlying network infrastructure. In this way home router can be smarter and all the network devices can be able to connect on a flat Ethernet, and there is no need to assign IP addresses to network devices. It is realized by the data center network designers that configuration complexity for a network of servers can be reduced by configuring as a single flat network, and it is easier to move servers from one portion to another portion of the network [13].

On the other hand, the designers of the enterprise networks also setup network as a single VLAN (virtual local area network) so that network devices can be moved from one point to another point seamlessly [1].

B) Network Maintenance

Connectivity Maintenance: not enough visibility:

After setting up the home networking, users need to know about the following:

1) In order to ensure that the proper functionality and security of devices, he may need to know the type of devices connected to network.

2) In order to determine how the task of these devices will be affected, he may need to know the level of performance, the devices received.

Now days, these tasks are very difficult. Although connected devices and user ISP connection status is enumerated by the router configuration page, but no action can be taken for this information. It is not indicated by the existing interfaces whether internet is reachable for a device to connect with, or if a device is configured with a wrong network, particularly in case of wireless connections [28]. Because router is a main monitoring point and control in the home networking, all the traffic passes through the router to the internet. Therefore router has all the information and situational awareness can be improved if router is better presented.

Visible connections improvement by restructuring the network:

A change in network infrastructure can be used to provide additional functionality to router. This functionality can be used to expose connectivity and performance information. More intuitive abstractions can be provided by home network user interface that helps in providing actionable information and situational awareness for external and internal connectivity.

Kermit study is an example of home network situational awareness improvement for the benefit of end users. According to this study, home network infrastructure can be easily managed by the users if home network devices could be associated with recognizable pictures and if network devices show their status as connected when they are actually connected to network [29]. This network interface helped users to see the status of device connectivity to network. It also helped to see the connection of unauthorized devices to the network. A user can block the access to an unauthorized device when it noticed its presence. Other interfaces can be enabled by restructuring the underlying network infrastructure. These interfaces can help in the improvement of situational awareness and actionable information. Bandwidth hogs can be revealed in home network by another system called Home Watcher [30].

In Home Watcher, situational awareness is improved because interface display is automatically configured with the network devices. A user can troubleshoot the connectivity problems in a better way because the system helps to provide actionable information. According to this type of system, if a device is configured properly with the router but it is facing connectivity issues, then it means that the problem in not in home network and a user can report to the ISP about the problem.

Home network infrastructure up gradation: Users of the home network spend a considerable amount of time in performing digital housekeeping because of the complexity in home network configuration management [5].

Users of the home network may be reluctant to change the existing network infrastructure because of the complexity in network configuration e.g. routers, access points. Reverting a network configuration change is very limited because of the complexity of network infrastructure. This inability to revert network configuration has made the possibility limited to revert the network topology or wiring to previous state in case of upgrade failure.

Reduce connectivity complexity by restructuring the network: Network configuration changes and upgrades are facilitated by restructuring the network into a single flat network. In a single flat network, because all network devices can communicate with each other, network physical topology can be changed by the user, without any fear of unknown dependencies. Without topological hierarchy, the changes remains to the network are device configuration changes and these changes can be managed by a central location such as router in the home network.
After all the changes in the network are limited to policy or device configuration at central point, a user can revert the state to previous state by reverting the single device state. Once these changes in network are revertible, these changes can be more visible to user by network interfaces. The task of network changes raises various questions about how this new functionality can be exposed to end users by network interfaces so that situational awareness can be improved and user actions can be enabled.

Shift network management task to third parties by restructuring the network: A single network infrastructure can be sliced into multiple virtual networks by network virtualization, an emerging network technology.

With the help of network slicing, we can think of network as many separate networks, each of these networks have its own services, network configuration and management [20]. A variety of new network functions are enabled by slicing the physical network infrastructure into multiple virtual networks. One possibility is that access to a slice of home network could be granted to ISP by the home user and ISP can perform remote network management and troubleshooting. An ISP could be provided with enough visibility to manage the home network, but an ISP has limited access to the home network user's private information. By using this approach, network complexity is moved from the home user but interfaces need to be co-designed to enable the remote management and troubleshooting.

IV. NETWORK PERFORMANCE

The usability of various network applications is greatly affected by the network performance.

Information about network performance provided by different ISP must be compared by users in setting home network. Home users expect a fully functional network in everyday operations. The network must support a wide range of operations such as email, browsing and video streaming and much more. Inadequate visibility is provided by home networks in network performance. Improvement in situational awareness related to network performance can be achieved by refactoring the network.

A) Network set up for optimal performance

Little visibility in choosing an internet service plan: An internet service plan must be chosen from provided ISP's by users to set up home network. A service plan must be selected by a user from an advertisement based ISP. This service plan must have concern about two metrics: connection speed and connection cost. Many aspects related to ISP performance are not visible in the advertisements of broadband. These aspects can greatly affect the user experience about online applications. After purchase, it is not currently possible to audit a plan.

Network performance monitoring is not supported by the current home network infrastructure even if other network aspects are visible. It is also not possible to report these statistics to users or any governing body.

Better measurements by restructuring the network: Network monitoring can be supported by restructuring the underlying network infrastructure, to reflect the performance of ISP. This information can be made visible so that situational awareness can be improved over time e.g., OpenWrt modules, these modules are running on router in the home network and can continuously measure the performance of network [11]. An ISP can advertise the access to home network performance if a user wanted to measure a wide range of performance metrics. After purchasing a specific service plan by the user, user can audit these metrics, and this information's can be made actionable, as plan can be changed by the user if it will not perform as required.

Following challenges are involved in providing intuitive network performance measurement:

1) Network metrics enumeration can affect the performance.

2) Metrics mapping to user friendly representations.

The first step is taken by the network researchers and proposed a raw set of network metrics. Application performance can be affected by these metrics. In the next step, these metrics are represented in more intuitive way. These low level metrics to measure performance can be mapped to meaningful metrics for application performance measurement. For example, it is very difficult to understand by the users how severe performance degradation can be introduced by packet loss in voice streams, While one can think to profile a user so that the applications commonly used in home can be identified and a performance report for these applications can be presented on the basis of low level metrics observation, e.g., Skype is performing poor, it is not necessary to tell the user that this poor performance may be due to higher loss of packets than application expects.

A novice user only needs to know that Skype is performing poorly, but additional insight is gained by the expert user by knowing the root cause. As an alternative approach, a low level performance metrics can be mapped to more intuitive visual representations that can be understood by the user, e.g. width of a pipe may represent the ISP connection downstream speed. Pipes of different lengths can be used to represent the latency.

B) Network performance auditing and troubleshooting

Little visibility in isolating the source of a performance problem: It is of great interest for network users and agencies to determine whether performance of internet service provider is according to the rates as advertised [22]. The home network and ISP network performance is not visible to users, It means users have no knowledge about network situational awareness and have limited information about the network functionality at any moment. Rather only end-to-end application performance view is visible to users, this view makes it difficult to isolate a network problem to a portion of network or device. It is difficult for the network users to diagnose the reason of network performance degradation because of the unavailability of suitable actionable information. Because of poor performance (slow internet), an ISP may get consumers service calls. This poor performance may be caused by the user's network configuration. It is difficult for the ISP to properly troubleshoot the performance issues without examining the home network.

Continuous visibility of ISP and home network performance by refactoring the network:

It is possible to collect and send reports to internet service providers and network consumers about network performance metrics by refactoring the network functionality. This refactoring makes it possible for the routers to measure performance. Situational awareness can be improved and actionable information can be provided to users by this approach and it helps the user to isolate network performance problem in a better way. If home router performs these measurements, then these can be much more accurate and there will be possibility of not affecting by the end user device [36].

BISmark [9] project, an open platform, can be used to measure performance of home network from routers. Home users privacy can be compromised when measuring the home network performance.

Improve performance visibility for ISPs by refactoring the network to benefit users:

Limited network performance measurements and diagnostics can be allowed by refactoring the network. In this way, visibility of the ISP can be improved for the home users. Home router is an ideal location for diagnostic platform because home network configuration and infrastructure may be changed continuously by the users.

An ISP can perform following diagnostics by using this platform:

1) Speed measurement of wireless network to home network devices.

2) Performance measurements of its own network, as is visible from home router.

Traffic traces for various specific applications can be captured by an ISP and it can also determine the exact location of problems about network performance, e.g. packet loss. It is a challenging task to provide situational awareness and actionable information to ISP without seriously compromising the user privacy, a user may not want to disclose and give access to ISP to the type of network devices connected to network. The information about the connected network devices can be helpful for users or ISP to diagnose the source of problem.

V. NETWORK POLICIES

The rules that control the flow of network traffic are called network policies.

A variety of factors may be encompassed by a policy such as access control, prioritization, rate limits and usage.

There are two types of policies:

1) Internal: this policy can be applied within the home.

2) External: this policy can be applied by an ISP to traverse the network.

We argue that too much visibility is provided by the home network infrastructure in setting up internal network policies, but not much visibility is provided in how ISP implements external policies. Better interfaces can be co-designed by refactoring policy related functionality into routers. This can help in setting and maintaining policy.

A) Network policies set up

Too much visibility in setting up home network internal policies: User's reactions will be positive in having control over prioritizing connections [30], [29], but this functionality setup is complicated because there is no separation between policy and mechanism provided by network interface. Users must configure low level mechanisms to specify high level policy.

Mechanisms for setting up these policies are too much complicated [15] that users never try to implement these policies in the first place, even though a wide variety of policies are available.

For example, user of home network want to give internet access to network guests, but want to restrict access to the network devices and files. Users might also want to set priorities for various types of activities [2].

The mechanisms used for specifying and implementing the network policy are too much complicated and users never touch them most of the time in first place, simply adopt all or nothing policy. Some of this complexity has been exposed to users by the previous designs, so that the awareness of network traffic can be improved [27] or access control policies can be set [3]. However, complex network interfaces will be resulted by exposing the low-level complex mechanisms to users. It is necessary to simplify the underlying mechanism to develop to usable interfaces.

B) Monitoring network policies

Little visibility in monitoring internal network policies:

Network users need user friendly interfaces to monitor usage after specifying the policies. These interfaces also enforce these policies. In order to determine whether network activity and usage comply with the specified policies, users need to monitor network activity. For example, a network user who is using capped bandwidth plan may need to monitor the amount of cap used and make sure that everybody remains in their allocation plan. The users also want to monitor the network usage to determine that the network traffic comply with the policies specified.

Make network policies more visible by restructuring the network:

In order to have measurement model for network performance, restructuring the network can make the policies known to home network as well. The concerns related to network policy force the interface designers to come across another question about the visibility, to which this information should be visible in home network, by keeping in mind the user privacy?

Previous studies about performance prototypes in home network supposed that aggregated information about connected network devices should be visible to home users, because home network users can isolate the causes of performance problem with the help of information about home network usage. According to these reports, some users (i.e., parents) want the rights to control network resources because of the social structures in the home while other users don't want. In all the cases, network interfaces should be designed in such a way that they can designate the users who have access to resources and information.

Little visibility in monitoring ISP and external network policies:

A little visibility about the ISP policies is provided by the existing network infrastructure, it can affect the performance of various applications [21]. Recently, internet service providers have implemented network policies that can block various applications traffic such as BitTorrent traffic. Network users are interested in network performance measurement delivered by internet service providers [22], also as the usage caps are provided by the ISP, users also want to measure how various applications and network devices consumes the allocation.

Internet service providers have no act of making the network policies visible to home users, so the users can discover from their network devices that policies are implemented by the ISP that can degrade some applications performance, but users cannot discover these policies because of the complexity in current network infrastructure.

Make external policies more visible by restructuring the network:

There is no mechanism for network user to monitor the home network's ISP side. The performance measurement model, we previously proposed, may permit the interfaces that can monitor policies, by providing information that can improve situational awareness and users can act on policy violations. This information's can be provided on ISP network operations.

VI. INTENTIONAL NETWORK INTERFACES

In the previous sections, it is explained how design decisions related to visibility can be enabled by changing the underlying network infrastructure that could improve interfaces for network performance and policy related tasks. It becomes clear from our examples that programmability is a network infrastructure property that contribute to the co-design of interfaces and applications. When restructuring home network infrastructure will not compromise the existing network functionality, then applications of users can be built on its main interfaces or additional monitoring can be supported by using refactoring. Control over underlying system behavior can be provided by restructuring the infrastructure, to support various requirements of application such as accountability, visibility and intelligibility.

This section will provide examples where networks and related interfaces can be co-designed.

We described various interfaces below, called the intentional interfaces, can help in the improvement of situational awareness and users could be provided with actionable information.

Infrastructure:

As previously described, an ISP can be provided with the ability to do remote maintenance or network troubleshooting on behalf of users by network virtualization. Although remote troubleshooting can be provided by the network restructuring, described above, but network interfaces for these tasks must be designed. Usable interfaces must be needed by network operators so that they can isolate home users performance problems from a remote central point.

Performance: Crowd Sourced ISP

Better visual ways must be needed by the ISP and home users to view the performance of broadband access networks so that the power relationship can be balanced among these stakeholders [21]. When a home user is facing a certain performance problem, they have a question in mind "Is the same problem occurs for other customers"?

An interface can be designed to allow users to not only monitor their network performance but also do a comparison with other user's network performance with same ISP. This interface can answer the above question.

The home network infrastructure, described above, where home users will be continually reported with performance information and measures, can be the basis of crowd sourced internet service provider. In the past, same concepts have been proposed, but end user devices performed the measurements, so these concepts faced the technical problems.

Policy: Bandwidth Brokers and Usage Meters

How much a user can be allowed to download before disconnection is limited by the usage quotas. Investigation of usage quotas suggest that better ways should be provided to users to monitor and control the usage over a billing cycle [31]. Utilization monitoring of various applications, network devices and users can be performed by home routers. A user can be allowed to cap with other home users by co-designing the interfaces. These interfaces help users to easily manage and monitor the usage caps, but this co-designing is an application design problem.

VII. RELATED WORK

Infrastructure: Infrastructure represents the building blocks and frameworks to support the user's everyday activities e.g. it may be roads, software systems, electricity grids. Until infrastructure breaks, it remains unnoticed [6], [7], [33].

Visibility in Networks: Belotti and Edwards [35] suggest that in order to improve the system's intelligibility and user understanding about the system's various actions, it is advisable to provide the visibility into system's internals. Similarly, in order to improve users' understanding of a system, the system should expose some metaphors that represent how the system is working [25]. The difficulties faced by the existing home network users were discussed in [5], [16], [18], [19]. Many of these difficulties are rooted in the network design infrastructure which was not created for home users [34].

Following approaches have been proposed by the researchers to address the difficulties in home networking.

1) Bandage approach: this approach helps in designing of interfaces to mask network complexity.

2) Clean Slate approach: it helps in the complete overhaul of internet protocols so that the protocols can be more user-centric [8].

Network Constraints Possibilities: Edwards et al. introduced a notation of constrained possibilities [23]. It suggested that it is possible to constrain the uses and interfaces of infrastructure at first place with its design. It is also suggested that changes in the underlying infrastructure are required when altering these constraints.

Network Monitoring and Control Point: Although connected devices and user ISP connection status is enumerated by the router configuration page, but no action can be taken for this information. It is not indicated by the existing interfaces whether internet is reachable for a device to connect with, or if a device is configured with a wrong network, particularly in case of wireless connections [28]. Because router is a main monitoring point and control in the home networking, all the traffic passes through the router to the internet. Therefore router has all the information and situational awareness can be improved if router is better presented.

Home Watcher: Bandwidth hogs can be revealed in home network by another system called Home Watcher [30]. In Home Watcher, situational awareness is improved because network devices automatically configured to the interface display. A user can troubleshoot the connectivity problems in a better way because the system helps to provide actionable information.

VIII. CONCLUSION

Network infrastructure for home networking is very complex. This infrastructure supports various network functions. Due to the complexity of infrastructure, home networking always remains challenging for users. Restructuring of the underlying network is possible by the recent developments in software defined networking (SDN) without affecting the existing network functionality. This paper showed where details about the underlying network are exposed too little or too much to the users to achieve their needs by current features of home networking. We also showed that restructuring the network can create the possibility for interfaces that can improve the situational awareness with actionable information for home users.

Finally examples of intentional interfaces are presented. These interfaces are built on restructured network and help to co-design of network interfaces. In this paper, the examples illustrate how programmability provided by software defined networking can help to co-design the network interfaces and infrastructure.

REFERENCES

[1]. M. Yu, J. Rexford, S. Xin, S. Rao, and N. Feamster. A survey of virtual lan usage in campus networks. IEEE Communications, 49(7):98–203, 2010.

[2]. Y. Yiakoumis, K.-K. Yap, S. Katti, G. Parulkar, and N. McKeown. Slicing home networks. In ACM SIGCOMM Workshop on Home Networking, Toronto, Ontario, Canada, Aug. 2011.

[3]. J. Yang and W. Edwards. Eden: Supporting home network management through interactive visual tools. In UIST, pages 109–118, New York, NY, 2010.

[4]. P. Tolmie, J. Pycock, T. Diggins, A. MacLean, and A. Karsenty. Unremarkable computing. In ACM CHI, pages 399–406, 2002.

[5]. P. Tolmie, A. Crabtree, T. Rodden, C. Greenhalgh, and S. Benford. Making the home network at home: Digital housekeeping. In ECSCW, Limerick, Ireland, 2007.

[6]. S. Star and K. Ruhleder. Steps towards an ecology of infrastructure: Design and access for large information spaces. Information Systems Research, 7(1):111–134, 1996.

[7]. L. Star. The ethnography of infrastructure. American Behavioural Scientist, 43(3):377–391, 1999.

[8]. E. Shehan and W. Edwards. Home networking and hci: What hath god wrought? In ACM CHI, 2007.

[9]. Project BISmark. http://projectbismark.net.

[10]. E. S. Poole, W. K. Edwards, and L. Jarvis. The home network as a socio-technical system: Understanding the challenges of remote home network problem diagnosis. Comput. Supported Coop. Work, 18(2-3):277–299, 2009.

[11]. Openwrt. https://openwrt.org/.

[12]. Network magic. http://www.purenetworks.com/product/pro.php.

[13]. R. N. Mysore, A. Pamboris, N. Farrington, N. Huang, P. Miri,S. Radhakrishnan, V. Subramanya, and A. Vahdat. Portland: a scalable fault-tolerant layer 2 data center network fabric. In ACM SIGCOMM, pages 39–50, Barcelona, Spain, Aug. 2009.

[14]. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. Openflow: Enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38(2):69–74, 2008.

[15]. M. Mazurek, J. Arsenault, J. Bresee, N. Gupta, I. Ion, C. Johns, D. Lee, Y. Liang, J. Olsen, B. Salmon, R. Shay, K. Vaniea, L. Bauer, L. Cranor, G. Ganger, and M. Reiter. Access control for home data sharing: Attitudes, needs and practices. Atlanta, GA, May 2010.

[16]. S. Kiesler, V. Lundmark, B. Zdaniuk, and R. E. Kraut. Troubles with the internet: The dynamics of help at home. Human Computer Interaction, 13:323–351, 2000.

[17]. N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker. Nox: towards an operating system

for networks. ACM SIGCOMM Computer Communication Review, 38(3):105–110, 2008.

[18]. R. E. Grinter, W. K. Edwards, M. Chetty, E. S. Poole, J.-Y. Sung, J. Yang, A. Crabtree, P. Tolmie, T. Rodden, C. Greenhalgh, and S. Benford. The ins and outs of home networking: The case for useful and usable domestic networking. ACM Trans. Comput.-Hum. Interact., 16(2):1–28, 2009.

[19]. R. E. Grinter, N. Ducheneaut, W. K. Edwards, and M. Newman. The work to make the home network work. In ECSCW, pages 469–488, Sept. 2005.

[20]. N. Feamster, L. Gao, and J. Rexford. How to lease the internet in your spare time. CCR, 37(1):61–64, 2007.

[21]. Measuring Broadband America: A Report on Consumer Wireline Broadband Performance in the U.S. Technical report, 2011. Federal Communications Commission.

[22]. Connecting America: The National Broadband Plan, 2010. Federal Communications Commission.

[23]. W. K. Edwards, M. W. Newman, and E. S. Poole. The infrastructure problem in hci. pages 423–432, Atlanta, GA, May 2010.

[24]. W. Edwards, V. Belotti, A. Dey, and M. Newman. Stuck in the middle: The challenges of user-centered design and evaluation for infrastructure. In ACM CHI, Ft. Lauderdale, FL, 2003.

[25]. P. Dourish. Accounting for system behaviour: Representation, reflection and resourceful action. In Computers in Context, Aarhus, Denmark, 1995.

[26]. A. Dey and A. Newberger. Support for context-aware intelligibility and control. In ACM CHI, Boston, MA, May 2009.

[27]. S. Consolvo, J. Jung, B. Greenstein, P. Powledge, G. Maganis, and D. Avrahami. The wi-fi privacy ticker: improving awareness and control of personal information exposure on wi-fi. In Ubicomp, pages 321–330, Copenhagen, Denmark, 2010. ACM.

[28]. M. Chetty, J. Sung, and R. E. Grinter. How smart homes learn: The evolution of the networked home and household. In Ubicomp. Springer-Verlag, 2007.

[29]. M. Chetty, D. Haslem, A. Baird, U. Ofoha, B. Sumner, and R. Grinter. Why is my internet slow?: Making network speeds visible. Vancouver, BC, Canada, May 2011.

[30]. M. Chetty, R. Banks, R. Harper, T. Regan, A. Sellen, C. Gkantsidis, T. Karagiannis, and P. Key. Who's hogging the bandwidth: The consequences of revealing the invisible in the home. Atlanta, GA, May 2010.

[31]. M. Chetty, R. Banks, A. J. Bernheim Brush, J. Donner, and R. E. Grinter. Under development: While the meter is running: computing in a capped world. interactions, 18:72–75, 2011.

[32]. K. L. Calvert, W. K. Edwards, and R. E. Grinter. Moving toward the middle: The case against the end-to-end argument in home networking. In ACM SIGCOMM Workshop on Hot Topics in Networking (HotNets).ACM, 2007.

[33]. G. Bowker and L. Star. Sorting Things Out: Classification and Its Consequences. MIT Press, 1999.

[34]. M. S. Blumenthal and D. D. Clark. Rethinking the design of the internet: the end-to-end arguments vs. the brave new world. ACM Trans. Internet Technol., 1(1):70–109, 2001.

[35]. V. Bellotti and W. K. Edwards. Intelligibility and accountability: Human considerations in context-aware systems. Journal of Human-Computer Interaction, 16(2-4):193–212, 2001.

[36]. S. Bauer, D. Clark, and W. Lehr. Powerboost. In ACM SIGCOMM HomeNets Workshop, Toronto, Ontario, Canada, Aug. 2011. ACM.

[37]. B. Aggarwal, R. Bhagwan, T. Das, S. Eswaran, V. N. Padmanabhan, and G. M. Voelker. Netprints: diagnosing home network misconfigurations using shared knowledge. In 6th USENIX Symposium on Networked Systems Design and Implementation (NSDI), pages 349–364, Boston, MA, 2009. USENIX Association.