HomeVisor: Adapting Home Network Environments

Tomasz Fratczak, Matthew Broadbent, Panagiotis Georgopoulos, Nicholas Race
School of Computing and Communications, Infolab 21,
Lancaster University, Lancaster, LA1 4WA, United Kingdom
{t.fratczak, m.broadbent, p.georgopoulos, n.race}@lancaster.ac.uk

***Abstract*—This paper considers SDN, and OpenFlow in particular, as technology to develop the next generation of more flexible, configurable and automated home networks. We identify the problems with the current state of the art in home networking, which includes a lack of user engagement in home network maintenance and configuration, Internet bandwidth limitations, and a lack of ISP reconfiguration and troubleshooting tools. We propose HomeVisor; a novel remote home network management tool. In this paper, we evaluate HomeVisor's ability to outsource control to an entity outside the home network. This includes the overhead of multiple slices within the home, and the effect of controller latency on network performance.**

I. Introduction

The popularity of domestic Internet access and the capacity of home broadband networks has steadily increased over the past two decades [1]. During this time, the nature of content available on the Internet and the underlying network infrastructure has evolved. Internet content is increasingly interactive and includes both bandwidth intensive and latency sensitive applications. Uses include video streaming and online gaming. At the same time, the home network itself has become an increasingly complex environment, integrating a range of networking hardware that has to satisfy the demands of users.

There are additional challenges within the home compared to other networks. This is an environment where users do not typically possess the skills [12] or wish to be burdened with the issues of home network management, configuration and troubleshooting [4]. The implications of this are often felt by ISPs, who have the responsibility of supporting their users, but often without direct control of the equipment within the home. This is compounded by a lack of tools to investigate the internal behaviour of a home network, with ISPs historically relying on costly call centre-based diagnosis [5]. Home networking clearly needs improving, particularly in respect to manageability, troubleshooting and performance optimisation. We believe that Software Defined Networking (SDN), particularly OpenFlow [10], has a role to play in addressing some of these issues.

OpenFlow, and more specifically FlowVisor [19], provides the ability to slice networks; with each slice accommodating traffic with different requirements, but also employing mechanisms to assure a certain quality of experience. By slicing a home network, there is an opportunity to consider how the management of these individual slices could be "outsourced". Each of these network slices could potentially be controlled separately by different service vendors that are specialised in optimising the delivery of their digital content. This allows the service providers to fine-tune delivery all the way to the network edge, without the need for any user involvement [21].

This paper introduces HomeVisor, a home network configuration and management tool. In particular, we focus on evaluating whether outsourcing the management of home network slices is viable, and assess the scalability and efficiency of such an approach. HomeVisor is designed to:

1) Enable remote home network troubleshooting and management.
2) Support fine-grained configurations closely suited to user requirements.
3) Provide a user agnostic and non-application centric approach.

The remainder of this paper is organised as follows. Section 2 provides the background of this work, including a discussion of current domestic network issues and other related work in the area. Section 3 introduces the design of HomeVisor, followed by the implementation in Section 4. An evaluation of HomeVisor is presented in Section 5 and finally, Section 6 concludes the paper.

II. Background

A. Domestic Network Problems

Over the last 15 years home networks have been transformed from 56kbps dial-up connections serving a single computer in the late 1990s, to always-on broadband connections, now available worldwide. In the UK, 63% of adults have access to fixed-line broadband services, with average Internet connection speeds of 12Mbit/s [1]. Nowadays, home networks serve personal computers, mobile phones, video game consoles, smart TVs and even home appliances. This represents a significantly more complex environment than just 10 years ago, incorporating a range of networking technologies and heterogeneous end-user devices sharing a limited broadband connection.

A users' knowledge of their network and its operation has not kept pace with technology. User studies show that people may struggle with the simplest of tasks [8], and often have to rely on the help of relatives and friends with more experience in the area [17].

Ethnographic studies, such as [17], show that home network management is universally problematic, and despite recent research efforts [3], [9], [11], [16], [21], there is little in terms of commercial applications that address this interface gap between home networking hardware and its users. Grinter et al. [6] notes that despite some technological similarities between a home network and a small, commercial office network, the

978-1-4799-2433-2/13 $31.00 © 2013 IEEE
DOI 10.1109/EWSDN.2013.12

behaviour of the network's users and their interaction with the computer and networking hardware varies greatly. Even though household members are essentially administrators of their own domestic network, they often neglect important tasks such as backups, upgrades and updates on their hardware and software. Chetty et al. [4] performed an ethnographic study that reveals a number of problems that UK households face with their home broadband connections and home networks in general. These are based on the residents' lack of network expertise. Due to the lack of understanding with the workings of their network, household members would develop their own, often mislead, theories about the reasons for which the home router or broadband connection does not provide the performance advertised. Troubleshooting would often be limited to rudimentary fixes, such asking other household members to release the network resources they were using, unplugging the router, or complaining to the ISP. Therefore, Chetty et al. [4] suggest that home network management should either be made easier or the responsibility taken away from users altogether.

One should not forget that there is a cost associated with hardware and service troubleshooting, and the customer support that accompanies this. A lack of understanding with domestic networks and the inability to successfully troubleshoot their problems not only impacts the user experience, but also increases the costs of technical support [5]. The statistics for hardware returns in home networks indicate that only 5% are actually related to a hardware fault [2]. Service providers are responsible for supporting their users and their home networks, often without the ability to access any information that would allow them to identify the fault.

B. Related Work

One of the steps taken to tackle the issues arising from misconfiguration and mismanagement, is to make diagnostic data from home networks available to ISPs and third parties. Calvert et al. [3] proposed a design for an OpenFlow-based universal logging platform, aimed at supporting diagnostics and troubleshooting problems in home networks. Their work concludes that the problems with home network troubleshooting is the lack of ability to identify what changed in the network at the moment of failure, and how the state of the network differs, before and after the problem-causing event. Home networks, as one of the edges of the Internet, conform to the standards that were created in the 1970s for the whole of the Internet, and carry over many of the assumptions that were made at the time. These include the belief that scalablility and end-to-end reliability remained high through trustworthy end-points managed by skilled administrators [20]. However, the same work notes that home networks are both highly heterogeneous and evolve over time. There is a lack of tools that can be used to give non-expert users the necessary understanding, allowing them to manage their own networks. They also highlight a growing interest in both the networking and HCI communities to address the aforementioned issues.

The "Homework" research project [7] has conducted a range of studies around home networks. This includes three studies focusing on mitigating home networking problems [11], [12], [20], and one addressing the needs of a home user [13].

Other work presents a new approach to dynamic traffic prioritization [9]. Martin and Feamster's study is an attempt to show that home networks can be designed around users, and therefore better suit their immediate needs.

Yakoumis et al. [21] provides a major influence to our work. They study the problem of inadequate home broadband speeds in the face of rapidly increasing online content consumption and argue that home networks are expensive to deploy, hard to manage and prone to failure. At the same time the authors claim there are no mechanisms or technology in place allowing ISPs to manage and improve home networks. Therefore, they propose slicing as a way to mitigate some of the problems home broadband users are faced with, by allowing multiple service providers (for example online video providers) to effectively share the infrastructure with limited impact on each others' share of the network.

III. Design

This paper introduces HomeVisor, a home network management tool. As mentioned previously, HomeVisor uses an existing tool developed for use with OpenFlow: FlowVisor [19]. FlowVisor acts as a hypervisor for OpenFlow networks, allowing logically separated slices to co-exist on the same set of physical hardware. These slices contain a subset of all network resources available. By slicing in this fashion, we can separate particular types of traffic into their own individual slice. It is this functionality that HomeVisor builds upon, and tailors specifically to a home networking environment. A slice can be created containing all, for example, TCP traffic. Greater granularity is also possible, such as slicing based upon HTTP traffic. Once a slice has been defined, it allows us to define the characteristics we want the traffic to conform to. Through the use of slicing, HomeVisor can provide:

1) Fast and fine-grained home network configuration through network slicing.
2) Quick creation and management of new and existing network slices.
3) Outsourcing control of these slices to other parties, including those located externally.

Figure 1 illustrates the main components of HomeVisor. It also demonstrates the interactions with the rest of the home networking environment. HomeVisor has three main components:

1) **Web User Interface**: provides a "front-end" control interface for the system. Through this, users can manage their network and upload new configurations.
2) **Network Management Component**: coordinates the other elements of HomeVisor, and acts as a gateway to the underlying OpenFlow software.
3) **XML API**: translates XML-based configuration setups for the support of fast and easy configuration and reconfiguration.

HomeVisor's environment is modular and flexible in terms of the placement of each of its components. These elements can be located at any point in a network. Figure 1 illustrates this layout. This approach also conforms with the SDN ideology of flexible placement and control. With this design, the four main elements can be located at different locations, such as in a user's home, in an ISP's infrastructure or even in a third-party provider's infrastructure. The modular nature of HomeVisor's architecture presents ISPs with the capability to troubleshoot and manage such home networks remotely. Furthermore, they can delegate control to trusted external bodies for improved efficiency and service-centric fine-grained configuration. The HomeVisor application interfaces with a FlowVisor instance to manage and configure a home network, managing slices and remote control of the network.

HomeVisor also requires minimal changes to the home network; additional functionality only relies upon the presence of an OpenFlow-enabled switch [10]. The actual home network topology, the way hosts are connected to the Internet and communicate, remains unchanged for the end user.

IV. Implementation

As discussed in Section III, HomeVisor is designed to be flexible in terms of where it is deployed. As such, we wanted to ensure it is also portable, so that it could be easily deployed on a range of systems. Therefore, much of HomeVisor is implemented in PHP.

HomeVisor's home network slicing mechanism utilises FlowVisor's functionality [18], with the aim of achieving the functionality we require. FlowVisor is not designed with home users in mind, who may have no or little experience of network administration. There is currently no graphical tools for managing a network or slice, something that inexperienced users would otherwise expect. HomeVisor presents a simple UI, which displays status information and facilitates automated configuration. HomeVisor also follows the Model-View-Controller (MVC) approach to software design, shown in Figure 3. This was chosen to allow the separation of concerns and facilitates the modularity and portability that the tool requires.

FlowVisor itself has both southbound and northbound APIs (Figure 2). The southbound interface is used to communicate with OpenFlow enabled hardware through the OpenFlow control protocol. Typically, this will be a number of hardware switches located throughout a network. The southbound interface also connects with one or more OpenFlow controllers. FlowVisor is used to define the resources that each controller has access to (i.e. a slice). In our home networking scenario, each slice will represent a particular type of traffic.

The northbound API exists to enable communication with other applications. We have taken advantage of FlowVisor's JSON API [14] in order to enable HomeVisor to monitor, control and visualise the network setup. We used the cURL library to connect to FlowVisor's RESTful API and parse the JSON requests and responses accordingly.

HomeVisor's XML API facilitates the creation of profiles and installation of network configurations. Each XML setup file contains a network setup profile, including all the necessary information required to correctly configure the network with any number of slices. The HomeVisor accepts these XML definitions and continues the process automatically. HomeVisor then translates the parameters contained in the XML files into FlowVisor API commands. As the example XML code below shows (Figure 4), through HomeVisor's XML API, we may specify a number of parameters used in the network. This includes defining how OpenFlow control messages should be handled or defining the location of controllers on a per-slice basis.

V. Evaluation

To evaluate the capabilities of HomeVisor, we considered a home networking scenario. In this scenario, we use HomeVisor to manage and control a testbed created to resemble a typical home network. The testbed consists of five Linux machines; a gateway, a controller and three host machines acting as

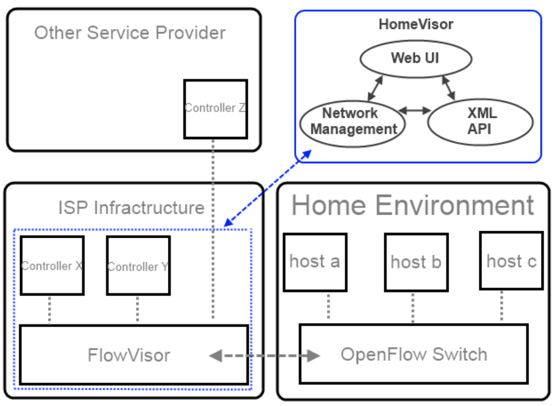

Fig. 1. High Level Design Overview

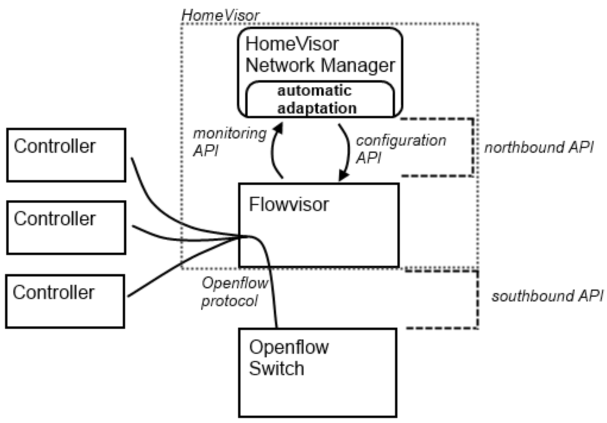

Fig. 2. HomeVisor Implementation

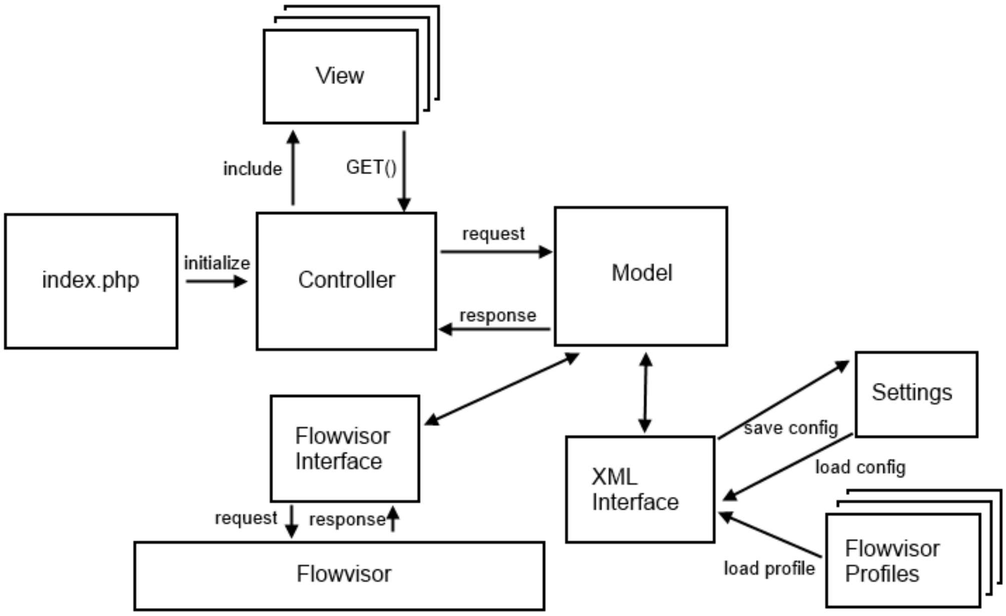

Fig. 3. HomeVisor Components and Interaction

```
<slice_name 'general_traffic'>
<controller_url>tcp:127.0.0.1:6634
</controller_url>
<admin_email>person@lancs.ac.uk
</admin_email>
<password>password</password>
<drop_policy>exact</drop_policy>
<receive_lldp>true</receive_lldp>
<flowmod_limit>-1</flowmod_limit>
<rate_limit>-1</rate_limit>
<admin_status>true</admin_status>
```

Fig. 4. Sample XML Configuration

user devices. The testbed also contains an OpenFlow-enabled switch (TP-Link TL-WR1043ND) running Pantou [15]. Utilising such an OpenFlow enabled switch provides a realistic hardware constraint synonymous with home networking equipment on the marketplace today. We ran HomeVisor on the control machine, and used the gateway to capture and analyse the incoming and outgoing Internet traffic for our tests. The outgoing link was limited to 12Mbit/s at the gateway to emulate a home networking scenario as accurately as possible [1].

To evaluate the performance of HomeVisor, we carry out tests using two scenarios. These are related to the specific configuration that might occur in a home network. The first aims to evaluate the scaling and performance of a slice based solution in a home-like network. The second aims to evaluate the effect of control to data plane latency, which might exist when we outsource the network management to an ISP or a third party, remote to the home network.

A. Slice Based Solution

Network slicing is an important network virtualisation mechanism provided through FlowVisor, which HomeVisor utilises to achieve multidimensional (across hosts, protocols, etc.) and fine-grained control over the home network resources. Therefore, we deemed it important to evaluate the impact that slicing has on the network performance. The results are included in this section.

The slice-based scenario involves running a series of tests (each repeated 10 times) where home-network-like traffic is produced. The overhead of HomeVisor is measured under heavy network load. This is created using multiple simultaneous BitTorrent downloads and playback of high-definition YouTube video streams. Traffic is captured at the gateway so that the incoming and outgoing Internet traffic is captured. We then use this to compare between the following three setups:

1) One network slice covering all of the traffic, controlled by a single controller. This is the control group.
2) Two network slices; one for low priority traffic (such as torrents and other downloads), one for the remainder of the traffic (such as video streams or VoIP).
3) Three network slices; one for non rate-limited low priority traffic, one for rate-limited low priority traffic and one for the remainder of the traffic (as above).

Table I shows the average packet delay variation that we measured for the three different slice setups. Notably, we observe in Figures 5 and 6 that when we introduce more slices, the traffic becomes more stable and we note less outlying packets with a high level of delay.

The positive impact of network slicing on the network

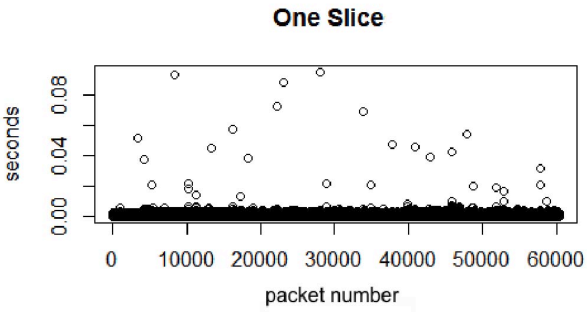

Fig. 5. Inter-packet delay measurements in one slice setup

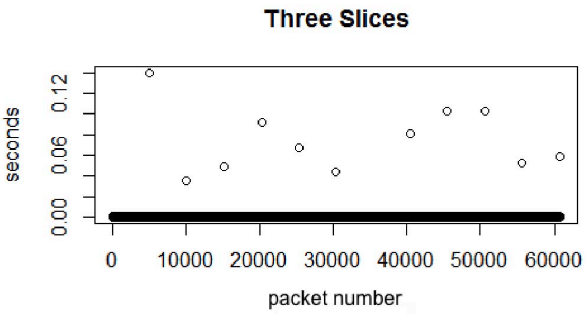

Fig. 6. Inter-packet delay measurements in three slice setup

performance was deemed statistically significant by t-test analysis:

- 1 slice versus 2 slices: t = 2.0227, p-value = 0.04311
- 1 slice versus 3 slices: t = 12.4415, p-value <2.2e-16

TABLE I
IMPACT OF SLICING ON PACKET DELAY VARIATION

# of Slices	Average Packet Delay Variation
1	0.001011110 sec.
2	0.001006057 sec.
3	0.000985257 sec.

B. Control Plane Latency

This section aims to quantify the effect of moving the control plane outside of the home network itself. The following evaluation will measure the impact of latency on the reaction time of the controller. This is particularly important as the control plane must be responsive to flow-level changes in order to avoid reducing responsiveness within the home network. The external location of the control plane will be emulated by introducing latency on two links: the Switch-to-FlowVisor link and the FlowVisor-to-Controller link. In the latter case, we create latency on both the links simultaneously.

We carried out four tests in a single-slice network setup with one OpenFlow controller. The latency levels on each of the aforementioned links are set to one of two levels; 0ms or 100ms. The latency of 100ms is set as an extreme value and is not necessarily representative of the kind of latency that would exist between a home user's switch and a controller within an ISP's infrastructure. However, it allows us to identify any problems that may arise in the case of unusually high latency or congestion within the network.

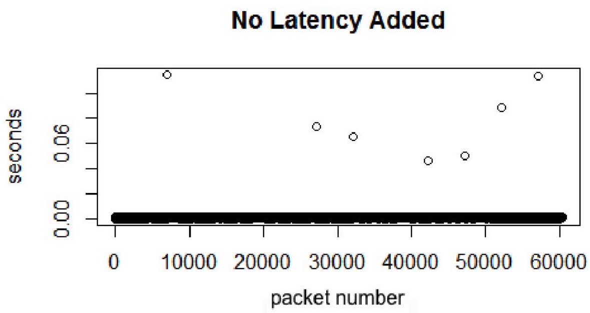

Fig. 7. Traffic behaviour when no additional latency is introduced between the data plane and the control plane.

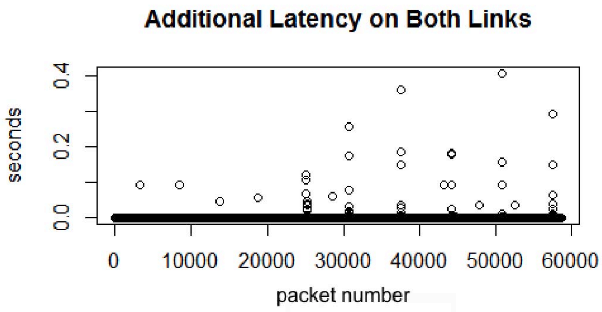

Fig. 8. Traffic behaviour when high latency is introduced between the data and control plane. 100ms is introduced between the switch and the FlowVisor and 100ms is introduced between the FlowVisor and the controller.

Figures 7 and 8 present the results of two of the tests. In particular, they present the packet delay variation where no latency is introduced, and where 100ms latency is introduced between both the Switch-to-FlowVisor link *and* FlowVisor-to-Controller link, respectively. The results of adding latency between Switch-to-FlowVisor or FlowVisor-to-Controller, but not both, are not included for brevity, although they are discussed here. The data analysis shows that latency between the home network data plane and its control plane does not affect the packet delay variation significantly, unless we introduce latency on both links (Figure 8). In fact, where added latency was introduced in one of the links, but not both, the average delay variation was marginally improved. We attribute this to FlowVisor receiving a low volume of control messages. The tests conducted with additional latency on both links show a more noticeable decrease in network performance (i.e. spikes in Figure 8), most likely caused by the delays in flow table modifications. Overall, the results show low packet delay variation, even in scenarios with added latency. This is an initial step in evaluating the feasibility of controlling a home network from a remote location.

VI. Discussion and Conclusion

In this work we have identified a lack of efficiency, management and troubleshooting in home networks. We have highlighted issues with the current state of the art, including an inability of ISP's to remotely troubleshoot or manage home networks, their non-user and non-application centric approach, and user disengagement from the configuration and management of their own networks.

We developed an OpenFlow-based prototype, the HomeVisor, to mitigate a subset of these problems. Further work is necessary to enhance the usefulness of the prototype by providing tools to more specifically troubleshoot and manage the home network. This is not a straightforward task, as considerations need to be made to tailor the interface and expose functionality to two potential stakeholders. These are as follows: a) customers using the home network and b) ISPs managing the home network. Clearly both stakeholders want to remedy these issues, but the level of control, proficiency, and experience need to be taken into account in both cases. Particularly in the case of home users, it is not apparent if a "one-size-fits-all" strategy would even be appropriate; further work is necessary in this respect.

Limitations of this prototype include an increased infrastructure requirement for ISPs. This is a result of provisioning the hardware to support the control platform, which will inevitably have to scale to serve a large amount of users. The cost of this hardware can be offset however against a reduction in direct support costs and staffing.

A further issue to note is the potential privacy concerns that might arise if the control of a network is done outside of the network itself. For example, communication, and subsequently control, could be hijacked by a malicious third-party. In this case, secure communications protocols, such as SSL, can be used to authenticate control traffic, and is already included within the OpenFlow specification. A further advantage of slicing the network is that by compromising a controller, an attacker would only control a single slice, limiting the potential damage to the scope of that slice.

The results of our tests, evaluating HomeVisor driven network slicing, demonstrate that network slicing can be used for fine-grained configuration and effective network management without negative impact on the core network performance. This can be achieved whilst running on a relatively cheap home-grade switching hardware. In fact, if our slicing approach is used in conjunction with an efficient control plane, it may actually improve the network's performance versus a standard single-slice design.

To summarise, we have concluded that home network control may be successfully outsourced without significant performance penalties, and even create potential benefits in optimisation and management of home networks by ISPs.

VII. Acknowledgments

This work is partially supported by EU FP7 funded project OFELIA (FP7-ICT-258365).

References

[1] Ofcom Facts and Figures. http://www.media.ofcom.org.uk/facts/, 2012.

[2] Accenture. Big Trouble with No Trouble Found: How Consumer Electronics Firms Confront the High Cost of Customer Returns, Jan. 2009.

[3] K. Calvert, W. Edwards, N. Feamster, R. Grinter, Y. Deng, and X. Zhou. Instrumenting Home Networks. *ACM SIGCOMM CCR*, 41(1):84–89, 2011.

[4] 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. In *28th International Conference on Human Factors in Computing Systems*, pages 659–668. ACM, 2010.

[5] W. Edward, R. Mahaja, and D. Wetherall. Advancing the State of Home Networking. *Communications of the ACM*, 54(6), 2011.

[6] R. Grinter, W. Edwards, M. Chetty, E. Poole, J. Sung, J. Yang, A. Crabtree, P. Tolmie, T. Rodden, and C. Greenhalgh. The Ins and Outs of Home Networking: The Case for Useful and Usable Domestic Networking. *ACM Trans. on CHI*, 16(2):8, 2009.

[7] Homework Project. Homework: user-centred home networking. http://homenetworks.ac.uk/.

[8] S. Kiesler, B. Zdaniuk, V. Lundmark, and R. Kraut. Troubles with the Internet: The Dynamics of Help at Home. *HCI*, 15(4):323–351, 2000.

[9] J. Martin and N. Feamster. User-driven Dynamic Traffic Prioritization for Home Networks. In *2012 ACM SIGCOMM Workshop on Measurements up the Stack*, pages 19–24. ACM, 2012.

[10] 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 CCR*, 38(2):69–74, 2008.

[11] R. Mortier, B. Bedwell, K. Glover, T. Lodge, T. Rodden, C. Rotsos, A. Moore, A. Koliousis, and J. Sventek. Supporting Novel Home Network Management Interfaces with OpenFlow and NOX. In *ACM SIGCOMM CCR*, volume 41, pages 464–465, 2011.

[12] R. Mortier, T. Rodden, T. Lodge, D. McAuley, C. Rotsos, A. Moore, A. Koliousis, and J. Sventek. Control and Understanding: Owning your Home Network. In *2012 Fourth International Conference on COMSNETS*, pages 1–10. IEEE, 2012.

[13] R. Mortier, T. Rodden, P. Tolmie, T. Lodge, R. Spencer, J. Sventek, A. Koliousis, et al. Homework: Putting Interaction Into the Infrastructure. In *25th Annual ACM Symposium on User Interface Software and Technology*, pages 197–206. ACM, 2012.

[14] OpenNetworkingLab. API Changes. http://github.com/OPENNETWORKINGLAB/flowvisor/wiki/API-Changes, February 2013.

[15] Pantou. OpenFlow 1.0 for OpenWRT. http://www.openflow.org/wk/index.php/Pantou_:_OpenFlow_1.0_for_OpenWRT.

[16] D. Pediaditakis, A. Gopalan, N. Dulay, M. Sloman, and T. Lodge. Home network management policies: Putting the user in the loop. In *Policies for Distributed Systems and Networks (POLICY), 2012 IEEE International Symposium on*, pages 9–16. IEEE, 2012.

[17] E. S. Poole, M. Chetty, T. Morgan, R. E. Grinter, and W. K. Edwards. Computer help at home: methods and motivations for informal technical support. In *Proceedings of the 27th international conference on Human factors in computing systems*, pages 739–748. ACM, 2009.

[18] R. Sherwood, G. Gibb, K. Yap, G. Appenzeller, M. Casado, N. McKeown, and G. Parulkar. Can the production network be the testbed? In *Proceedings of the 9th USENIX conference on Operating systems design and implementation*, pages 1–6. USENIX Association, 2010.

[19] R. Sherwood, G. Gibb, K.-K. Yap, G. Appenzeller, M. Casado, N. McKeown, and G. Parulkar. Flowvisor: A network virtualization layer. *OpenFlow Switch Consortium, Tech. Rep*, 2009.

[20] J. Sventek, A. Koliousis, O. Sharma, N. Dulay, D. Pediaditakis, M. Sloman, T. Rodden, T. Lodge, B. Bedwell, and K. Glover. An Information Plane Architecture Supporting Home Network Management. In *2011 IFIP/IEEE International Symposium on IMM*, pages 1–8. IEEE, 2011.

[21] Y. Yiakoumis, K. Yap, S. Katti, G. Parulkar, and N. McKeown. Slicing Home Networks. In *2nd ACM SIGCOMM Workshop on Home Networks*, pages 1–6. ACM, 2011.