Control and Understanding: Owning Your Home Network

C. Rotsos, A.W. Moore
Computer Laboratory
University of Cambridge

R. Mortier, T. Rodden,
T. Lodge, D. McAuley
School of Computer Science
University of Nottingham

A. Koliousis, J. Sventek
School of Computer Science
University of Glasgow

ABSTRACT

A rising proportion of the world's population uses, and thus must manage, wireless home networks. Unfortunately, these have evolved using protocols designed for backbone and enterprise networks, which are quite different in scale and character to home networks. We believe this evolution is at the heart of widely observed problems experienced by users operating and using their home networks. In this work we investigate redesign of the home router to exploit the distinct social and physical characteristics of the home.

We extract two key requirements from a range of ethnographic studies: users desire greater understanding of and control over their networks' behaviours. In order to fulfil these requirements, we develop a prototype router for home networks, build on top of NOX and OpenVSwitch, that provides per-flow control of traffic and uses a custom DHCP implementation to enable traffic isolation and accurate measurement from the IP layer.

1. INTRODUCTION

Consumer broadband Internet access is a critical component of the digital revolution in domestic settings: for example, Finland has made broadband access a legal right for all its citizens.[1] In parallel, a growing number of services are now provided over the Internet, while the number of IP-enabled devices in a household increased significantly the recent years leading to a wider usage on in-home wired and wireless networking. Despite the growth in Internet use and the explosion of interest in home networking, the opacity of networking technologies has meant they remain extraordinarily difficult for people to install, manage, and use in their homes. Many empirical studies in recent years have explored the clear mismatch between current networking technology and the needs of the domestic setting [5, 3, 1].

At the core of this problem we identify two main problems. Firstly, core network protocol and design principles were designed in the 1970's in order to cover the requirements of backbone and enterprise networks and having in mind a specific set of users. In contrast, home networks tend to be smaller in size and cooperatively self-managed by residents who are seldom expert in networking technology. As a result of these differences, simple management tasks may become technically prohibitively difficult.

[1] http://www.bbc.co.uk/news/10461048

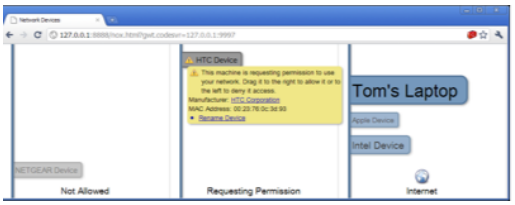

Figure 1: Control panel.

Secondly, the layered nature of current TCP/IP stack leads to a mismatch to the way people perceive network. Simply creating a user interface layer for the existing network infrastructure will only reify existing problems. Rather, we need to investigate creation of new network architectures reflecting the socio-technical nature of the home by taking into account both human and technical considerations.

In this work we are focusing in exploiting human understandings of the local network and the home to guide the management of the supporting infrastructure [1]. We transform the home router from a boundary point of an edge network into a physical device which can be exploited as a point of enriched and user-friendly management of the domestic infrastructure. In order to achieve that we exploit the extensibility that the OpenFlow protocol provides and develop a custom router network stack. Currently, our router design provides user friendly fine grain access control on the network and we are working towards extending this functionality to provide a richer management experience for users.

2. REDESIGN THE NETWORK STACK

Our home router is based on Linux 2.6 running on a micro-PC platform with access point functionality, provided by the *hostapd* package. The software infrastructure on which we implement our home router network

functionality consists of a NOX controller using a set of custom modules to control traffic and export a rich RPC API, the Open OpenVSwitch OpenFlow implementation, plus the Homework Database [4] providing an integrated network monitoring facility. On top of the network infrastructure we develop interfaces such as the Guest Board (Figure 1) to enable *ad hoc* control of network. This sort of control mechanism is a much more natural fit to the local negotiation over network access and use that takes place in most home contexts.

In order to support the functionality of our network design we introduce, using the NOX platform, the following switching and protocol modifications:

Address Allocation: We allocate each device its own /30 IP subnet. This way we force inter-device traffic to be IP routed via our home router, ensuring that all network traffic is visible to the router even in the case of shared layer 2 medium, like wifi.

Flow-level traffic control: Unlike current home routers, we exploit the capabilities of OpenFlow and develop a packet forwarding mechanism based on flows. This way we are able to exercise per flow access control, based on the policy that home users express.

Internet access control: In order to allow users to control Internet access, we implement a DNS aware NOX module that intercept DNS traffic and filters requests for specific domains. This way users are able to deploy access control policies based on domain names, a more intuitive service representation.

Medium Access Control: In order to secure the wireless network from security attacks, like eavesdropping, we use EAP-WPA2 encryption in our wireless medium. This design choice enables as to further control the medium utilisation by filtering WPA key exchange traffic. Thus the router is able to fully disconnect misbehaving nodes.

In order to evaluate our design, we focus on two important performance aspects: heterogeneity and scalability. For the case of heterogeneity, we tested our design against a wide range of IP-enabled devices and we ensured that it provides seamless connectivity to all devices and supports all protocols (e.g. UPnP, skype). Additionally, by using the linux kernel packet generator [2], we emulated a variable number of flows and hosts generating traffic at wire speed (100Mbps). We observed that the router modified network stack performs better than the standard Linux stack for small number of hosts and flows, while the switching and throughput performance scales linearly, as we increase the numbers. Furthermore, by using a modifies version of our router we logged network traffic of two typical households for a period of one month and compare the flow and host statistics with the results of our benchmark test. We conclude that our design incurs minimum impact on the performance of the router in a realistic environment.

3. CONCLUSIONS AND FUTURE WORK

By drawning upon previous user studies of home networks, we focus our research on the distinct nature of the setting and its implications. We introduce a new network design that, by exercise a number of protocol modifications, simplifies to a great extend the way home user can exercise fine level control on the traffic of their networks, with minimum impact on performance and device support.

Furthermore, because of the fine level of control and programmability that the OpenFlow protocol provides, we are currently working towards extending the functionality of the initial router design. Our exploration suggests that, just as with other edge networks, existing presumptions could usefully be reexamined to see if they still apply in this context. One of these presumptions, is the requirement of network neutrality on the home network. Such environments contain hierarchical relations between hosts, which currently are impossible to be expressed in traffic routing. We are currently interested to develop functionalities that allow users to express these relationships in a seamless way. Such information, can be shared additionally with service providers, through a framework that does not violate end-user privacy. Thus, service providers can reduce some of the traffic engineering effort by collaborating with end users.

4. REFERENCES

[1] A. Crabtree, T. Rodden, T. Hemmings, and S. Benford. Finding a place for ubicomp in the home. In *Proceedings of UbiComp*, pages 208–226, Seattle, WA, USA, Oct. 12–15 2003. Springer.

[2] R. Olsson. *pktgen*, the linux packet generator. In *Proc. Linux Symposium*, volume 2, pages 11–24, Ottawa, ON, Canada, July 20–23 2005.

[3] T. Rodden, A. Crabtree, T. Hemmings, B. Koleva, J. Hunble, K.-P. Akesson, and P. Hansson. *Assembling connected cooperative residential domains*, pages 120–142. Springer, 2007. In *The Disappearing Computer: Interaction Design, System Infrastructures and Applications for Smart Environments* (eds. Streitz, N., Kameas, A., and Mavrommati, I.).

[4] J. Sventek, A. Koliousis, O. Sharma, N. Dulay, D. Pediaditakis, M. Sloman, T. Rodden, T. Lodge, B. Bedwell, K. Glover, and R. Mortier. An information plane architecture supporting home network management. In *Proceedings of Integrated Management (IM)*, 2011.

[5] P. Tolmie, A. Crabtree, T. Rodden, C. Greenhalgh, and S. Benford. Making the home network at home: digital housekeeping. In *Proceedings ECSCW*, pages 331–350, Limerick, Ireland, Sept. 24–28 2007. Springer.