

# Domesticating Home Networks



UNITED KINGDOM • CHINA • MALAYSIA

Anthony Brown

School of Computer Science

The University of Nottingham

A thesis submitted for the degree of

*Doctor of Philosophy*

July 2016

---

## Abstract

This thesis addresses the following question: How should domestic networks be reinvented to support self-management by domestic users? It takes a user-centred design approach to redesign the underlying domestic network infrastructure to better fit domestic users. The overall aim of this work is to create user-centred mechanisms to support self-management of domestic networks by domestic users. Two areas of the domestic network are studied in detail, user-centred mechanisms for domestic network infrastructure control and user-centred presentations of network data.

User-centred mechanisms for domestic network infrastructure control are explored to improve Wi-Fi device association in domestic environments. A user-centred design approach is adopted to create a new method for sharing Wi-Fi credentials between devices, specifically tailored for domestic environments called MultiNet. The network performance impact of MultiNet is quantified using the standard metrics of throughput, latency, and jitter in a lab based experiment. MultiNet's usability is then compared to Wi-Fi Protected Setup in a lab based usability evaluation. These show that better Wi-Fi device association methods targeted for domestic environments can be built. It also shows that user-centred networking infrastructure can support self-management by domestic users.

User-centred presentations of network data address the poor legibility of domestic networks hinders configuration and maintenance of them. A user-centred approach is adopted to design and construct a network data visualisation and annotation platform, HomeNetViewer. Through a series of deployments in real households the

---

HomeNetViewer platform is used to explore user-centred presentations of network data to support the local negotiation of domestic network policy. HomeNetViewer improves domestic network legibility by enabling the construction of user-centred presentations of domestic network data. Additionally, it shows that users are comfortable annotating their network data using activities, applications, and users as a vocabulary. Together this highlights, with the correct user-centred tools, that domestic users are able to gain new insight into their networks to support self-management. HomeNetViewer also shows that manually annotating domestic traffic place an ongoing burden on the users.

Automating user-centred presentations of network data are explored to address the burden the annotation process places on users. The use of enterprise traffic classification techniques to generate user-centred presentations of network data struggle to classify the data annotated by HomeNetViewer participants. It concludes by suggesting two ways in which these difficulties could be addressed in future work.

Overall the domestic access point provides an important point of configuration, visibility and control over the domestic network infrastructure. This dissertation demonstrates that taking a user-centred design approach to reinventing the domestic network, to support self-management by users, can resolve the existing problems and merits further research and exploration by industry and standardisation bodies.

## Acknowledgements

My sincere thanks go to my supervisor, Prof Tom Rodden and Dr Richard Mortier. Thank you for your guidance and your wisdom during these last five years. I would also like to acknowledge The University of Nottingham and the RCUK Digital Economy programme their financial support which made this all possible. In particular, I would like to thank the staff and students in the Doctoral Training Centre for sharing and enriching the PhD experience.

This thesis is dedicated to my children Zach and Sophie. You have made me stronger, better and more tired than I could have ever imagined. Your thirst for knowledge and endless curiosity is an inspiration. My wife, Beth also deserves a special thank you. Her endless patience, unwavering belief, organisational skills and ability to make me laugh helped me through the most challenging times. The continued support and encouragement provided by my wider family and friends was also invaluable throughout.

Finally, I would like to thank my participants. Without your trust and kindness this work would not have been possible. Thank you.

# Contents

<b>Contents</b>	<b>i</b>
<b>List of Figures</b>	<b>iv</b>
<b>List of Tables</b>	<b>vi</b>
<b>List of Publications</b>	<b>vii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 User-centred mechanisms for domestic network infrastructure control	4
1.2 User-centred presentations of network data . . . . .	6
1.3 Automating user-centred presentations of network data . . . . .	7
1.4 Thesis structure . . . . .	8
<b>2 Background</b>	<b>9</b>
2.1 Domestic networks . . . . .	9
2.2 The domestic context of networks . . . . .	13
2.3 Domestic network challenges . . . . .	16
2.4 Addressing the challenges . . . . .	19
2.5 Wi-Fi device association . . . . .	22
2.6 Legibility of domestic networks . . . . .	25
<b>3 User-centred mechanisms for domestic network infrastructure control</b>	<b>31</b>
3.1 MultiNet design . . . . .	32
3.2 MultiNet implementation . . . . .	34
3.3 MultiNet usability analysis . . . . .	46

3.3.1	Participants . . . . .	46
3.3.2	Method . . . . .	47
3.3.3	Results . . . . .	49
3.4	Network performance . . . . .	52
3.4.1	Method . . . . .	52
3.4.2	Results . . . . .	52
3.5	Device connection time . . . . .	55
3.6	Discussion . . . . .	56
3.7	Limitations . . . . .	61
<b>4</b>	<b>User-centred presentations of network activity</b>	<b>62</b>
4.1	System design . . . . .	64
4.1.1	Ethical considerations . . . . .	67
4.1.2	Prototype interface . . . . .	69
4.1.3	Iterative design with home-owner . . . . .	71
4.1.4	Test deployment . . . . .	74
4.2	The final system . . . . .	76
4.2.1	Interactive visualisation . . . . .	76
4.2.2	Annotation capabilities . . . . .	76
4.3	HomeNetViewer deployment . . . . .	81
4.3.1	Method . . . . .	82
4.3.2	Participating households . . . . .	83
4.3.3	Results: data annotations . . . . .	85
4.3.4	Results: exit interviews . . . . .	85
4.4	Discussion . . . . .	94
4.5	Limitations . . . . .	98
<b>5</b>	<b>Automatic generation of user-centred presentations of network activity from IP Flow records</b>	<b>102</b>
5.1	Performance metrics . . . . .	103
5.2	Dataset and classes . . . . .	105
5.3	Classification algorithm and feature selection . . . . .	107
5.4	Results . . . . .	111

5.4.1	Household 1 . . . . .	115
5.4.2	Household 2 . . . . .	117
5.4.3	Household 3 . . . . .	120
5.4.4	Household 4 . . . . .	120
5.5	Discussion . . . . .	123
<b>6</b>	<b>Conclusion</b>	<b>125</b>
6.1	Key lessons . . . . .	125
6.1.1	User-centred mechanisms for domestic network infrastruc- ture control . . . . .	125
6.1.2	User-centred presentations of network activity . . . . .	126
6.1.3	Automatic generation of User-centred presentations from IP Flow records . . . . .	127
6.2	Open challenges . . . . .	128
6.2.1	User-centred mechanisms for domestic network infrastruc- ture control . . . . .	128
6.2.2	User-centred presentations of network activity . . . . .	128
6.2.3	Automatic generation of User-centred presentations from IP Flow records . . . . .	129
6.3	Next steps . . . . .	130
	<b>References</b>	<b>132</b>

# List of Figures

3.1	Overview of MultiNet implementation. . . . .	36
3.2	MultiNet <i>Network Controller</i> interface. . . . .	37
3.3	MultiNet interactions to add a device [16]. . . . .	39
3.4	Laptop client device with MultiNet QR Code encoded credentials. . . . .	42
3.5	Instructions for adding the printer to the network for WPS (top) and MultiNet (bottom). . . . .	48
3.6	Evidence for the learnability of MultiNet. . . . .	51
3.7	Device to access point network performance as the number of configured networks increases. The mean $\pm$ standard error is shown . . . . .	53
3.8	Average device connection time (s). . . . .	55
4.1	A system overview of HomeNetViewer data collection and annotation platform. . . . .	77
4.2	Final annotation interface for a single device. . . . .	78
4.3	Host/domain annotation interface . . . . .	79
4.4	One day's annotated traffic combined (all devices) in household 1 . . . . .	86
4.5	One day's annotated data for a shared device in household 1 . . . . .	100
4.6	An example of the visibility of H2U4s' daily routine and unknown traffic at odd times of night . . . . .	101
5.1	Classifier performance H1UT dataset . . . . .	109
5.2	Classifier performance H1AT dataset . . . . .	110
5.3	Classifier performance H1UT dataset with increasing number of estimators . . . . .	112
5.4	Classifier performance H1AT dataset with increasing number of estimators . . . . .	113



## LIST OF FIGURES

---

5.5	H1UV confusion matrix . . . . .	116
5.6	H1AV confusion matrix . . . . .	116
5.7	H2UV confusion matrix . . . . .	118
5.8	H2AV confusion matrix . . . . .	118
5.9	H3UV confusion matrix . . . . .	121
5.10	H3AV confusion matrix . . . . .	121
5.11	H4UV confusion matrix . . . . .	122

# List of Tables

3.1	Prior exposure to WPS and QR Codes. . . . .	47
3.2	User trial participant age range. . . . .	47
4.1	Household 1 participant information . . . . .	84
4.2	Household 2 participant information . . . . .	84
4.3	Household 3 participant information . . . . .	84
4.4	Household 4 participant information . . . . .	84
4.5	Annotations entered per household per annotation type . . . . .	85
5.1	Description of the Flow data collected . . . . .	106
5.2	H1UV classification results, optimistic precision shown in () . . .	115
5.3	H1AV classification results . . . . .	115
5.4	H2UV classification results, optimistic precision shown in () . . .	119
5.5	H2AV classification results . . . . .	119
5.6	H3UV classification results, optimistic precision shown in () . . .	120
5.7	H3AV classification results . . . . .	120
5.8	H4UV classification results, optimistic precision shown in () . . .	122

# List of Publications

- [1] Brown, A., Mortier, R., and Rodden, T. Multinet: Reducing interaction overhead in domestic wireless networks. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (New York, NY, USA,2013), CHI 13, ACM, pp. 1569-1578
- [2] Brown, A., Mortier, R., and Rodden, T. An exploration of user recognition on domestic networks using netflow records. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (2014), UbiComp 14 Adjunct, ACM, pp. 903-910.

# Chapter 1

## Introduction

This thesis addresses the following question: How should domestic networks be reinvented to support self-management by domestic users?

Empirical studies have highlighted many issues with currently deployed domestic networks. How they are supported, maintained, and expanded have been shown to be problematic. These problems have been the focus of much research within the Human Computer Interaction community (HCI) over the past 10 years.

Many attempts to address the problems found within domestic networks, focus solely on improving the user interface to the network, adding a layer of “interface veneer” on top of the complex underlying network infrastructure. This approach has had limited impact on commercially available domestic networking hardware. The usability of currently available domestic networking equipment is still problematic.

This dissertation argues that the root cause of many domestic network usability problems is the transplantation of the complex underlying networking protocols from corporate environments to the home. Networking protocols have migrated from corporate environments to domestic environments with little or no consideration for the domestic context, its users, or their goals.

Users are often faced with complex technical interfaces when performing basic network tasks. While better user interfaces may improve the situation, they cannot fully solve the usability problems inherent in today’s domestic networks in isolation.

---

This dissertation explores another direction, taking a user-centred design approach to redesign the underlying network infrastructure. The overall aim of this work is to create user-centred mechanisms to support self-management of domestic networks by domestic users, reinventing the networking infrastructure as required.

A case study style approach is taken to unpack the overarching question of this dissertation. Each case study will focus on one particular usability problem within domestic networks. The problems that will be tackled are identified by reviewing the existing literature on domestic network usability. A user-centred approach is adopted in each case study with the aim of reinventing the supporting domestic network infrastructure to support self-management by users.

Before continuing it is worth considering, why do domestic networks need to be reinvented? After all, domestic networks are now commonplace, and have become an unremarkable feature of everyday life [24]. Domestic networks are routinely used to access a vast array of content and services on a daily basis. Despite their widespread deployment the management, configuration, and control of this domestic resource imposes a significant technical burden on their users [13, 29, 79].

Domestic networks are built using a host of protocols, tools, and technologies designed for use on the wider Internet and in enterprise networks. These protocols were created assuming the presence of trained professional network engineers to configure and maintain them. In contrast, users of domestic networks are not usually trained networking professionals, and are not motivated to acquire the necessary skills. The documented issues with current domestic network deployments are reviewed in detail in Chapter 2.

Previous approaches to addressing domestic network usability have assumed that the underlying network infrastructure is immutable, only focusing on improving their user interface. However, recently a new approach to domestic network research has emerged. Edwards et al., first highlighted the need for HCI researchers to engage pro-actively with the development of networking infrastructure in 2010 [31]. Since then a small number of researchers have begun to explore the benefits of altering the domestic network infrastructure.

Mortier et al., have shown, that by carefully altering the configuration of the underlying network protocols new possibilities for user interaction can be

---

created [63]. Chetty et al., have explored exposing network bandwidth usage to domestic users on situated displays, and have shown it to be beneficial [20].

It is upon this work that this dissertation aims to build, by taking a user-centred design approach to reinventing parts of the domestic network infrastructure. It is not proposed to create a whole new set of protocols specifically for domestic environments. Changing them, adding new features, and altering how they are deployed and/or used to create domestic specific solutions is a key aspect to this work.

The three areas that the case studies will explore are: User-centred mechanisms for infrastructure control, User-centred presentations of network activity and Automating user-centred presentations of network data. These areas are very different, each has its own challenges, and they are best evaluated using different methods. Hence, a mixed methods approach to evaluation is adopted, selecting the most appropriate evaluation techniques as required. However, the case studies are explored using the same underlying approach: user-centred design.

It has been long established that user-centred design helps create useful, usable, and desirable products through an early focus on user requirements. User-centred design was first described by Donald Norman in 1986 thus:

“user-centred design emphasizes that the purpose of the system is to serve the user, not to use a specific technology, not to be an elegant piece of programming. The needs of the users should dominate the design of the interface, and the needs of the interface should dominate the design of the rest of the system.” [64]

The generally accepted principles of user-centred design are: an early focus on users and tasks, empirical measurement, and iterative design [35]. This is further expanded by Preece et al., who suggest adding five principles to clarify “an early focus on users” [73]. These are:

- 1 Users’ tasks and goals are the driving force behind development.
- 2 The system should be redesigned to support users’ behaviour and context-of-use.

- 
- 3 Users' characteristics are captured and designed for.
  - 4 Users should be consulted throughout development cycle and their input should be seriously taken into account.
  - 5 All design decisions are taken within the context of the users, their work and their environment.

These five principles place the user at the centre of the design process. However, this does not mean that the users make all the design decisions, but rather, that the designer should remain aware of the user requirements when making design decisions. Preece et al., also suggest that providing an accessible set of data about user requirements can help designers focus on users' needs. The focus of user-centred design on the users' tasks and goals within their context and environment is an ideal lens, through which to explore the issues of domestic network usability.

Thus, the underlying approach adopted, is to apply user-centred design to build a number of technology probes [43]. An analysis of the relevant literature and the domestic context is used to guide the design of the technology probes. They are then employed as a tool to elicit user feedback and test the technical limitations of our alterations, using the most appropriate method. Lab based experiments and a number of quantitative methods are used to measure the efficiency and effectiveness of our systems. These are complemented by real world deployments and qualitative methods to collect and report user feedback. Next, more detail is provided describing each case study.

## **1.1 User-centred mechanisms for domestic network infrastructure control**

Building, configuring, and repairing domestic networks is a complex task. When users wish to setup a new, fix a problem with, or add devices to an existing network, they are forced to interact with the complex underlying network infrastructure. This interaction can take many forms: web interfaces, operating system dialogues, and physical interaction are all supported modalities.

---

The protocols used in domestic networks were not designed with unskilled domestic users in-mind. The mismatch in knowledge and skills makes the task of constructing and modifying networks time consuming, and frustrating for most users. This section of the dissertation explores taking a user-centred approach to redesigning domestic network infrastructure to support user-centred mechanisms for infrastructure control.

One aspect of infrastructure control is selected to study in detail, namely, Wi-Fi device association. Wi-Fi device association is a particularly problematic interaction with domestic network infrastructure. It involves making security related decisions and entering security related information in a variety of different ways.

Improving Wi-Fi device association has been the focus of many academic studies. However, it is still one aspect of domestic network configuration that causes significant frustration for domestic users. To further understand what it means to build a user-centred mechanism for Wi-Fi device association in domestic environments, several sub questions will be explored. These are:

- Q2.0** Are User-centred mechanisms for infrastructure control beneficial for domestic networks?
- Q2.1** How should Wi-Fi device association be changed to better fit domestic environments?
- Q2.2** How much do the underlying protocols involved with Wi-Fi device association need to be changed to better fit domestic environments?
- Q2.3** What are the network performance implications of the redesigned infrastructure?
- Q2.4** How does the usability of the new method compare to existing device association methods?

These questions are addressed in Chapter 3. A user-centred design approach is adopted to create a new method for sharing Wi-Fi credentials between devices, specifically tailored for domestic environments. Question 2.0 is addressed



---

by reviewing the existing literature on usability issues with, and suggested improvements to, the Wi-Fi device association process. This literature review is then used to draw-up a set of design principles for the development of a new association method.

The design principles are then used to implement a new system which conforms to them, called MultiNet [16]. The modifications made to existing Wi-Fi device association protocols in the construction of MultiNet are documented to answer question 2.2. Question 2.3 is then covered by assessing the impact of MultiNet on network performance using the standard metrics of throughput, latency, and jitter in a lab based experiment. The usability of MultiNet is then compared to Wi-Fi Protected Setup (WPS), the current state-of-the-art in usable device association. The usability comparison of MultiNet and WPS is assessed using a lab based user study and semi-structured interviews. The results of the usability studies are presented to answer question 2.4.

Chapter 3 shows, that by taking a user-centred approach, better Wi-Fi device association methods targeted for domestic environments can be built. It also shows that user-centred networking infrastructure can support self-management by domestic users.

## 1.2 User-centred presentations of network data

The literature review shows that poor legibility hinders configuration and maintenance of domestic network infrastructures. Improving domestic network legibility is an important problem to address. Improving legibility also has applications in supporting the local negotiation, monitoring and enforcement of domestic network policies. This section of the dissertation looks at how user-centred presentations of network data can be used to improve domestic network legibility to support self-management by domestic users. It addresses four important questions:

**Q3.0** Do user-centred presentations of network data improve network legibility?

**Q3.1** Of the data flowing through the domestic network access point, which are best suited for use in user annotation?

---

**Q3.2** Are interactive time-series historical visualisation appropriate in the context of domestic network data?

**Q3.3** Is the use of activities, applications and users an appropriate language to annotate domestic network data?

**Q3.4** How do users feel about the increased network legibility?

To explore the questions above, a user-centred approach is adopted to design and construct a network data visualisation and annotation platform, HomeNetViewer [17]. HomeNetViewer is specifically designed for use in domestic environments by non-expert users. Through a series of deployments in real households the HomeNetViewer platform is used to explore user-centred presentations of network data to support the local negotiation of domestic network policy.

Chapter 4 shows that HomeNetViewer improves domestic network legibility by enabling the construction of user-centred presentations of domestic network data. Additionally, it shows that users are comfortable annotating their network data using activities, applications, and users as a vocabulary. Together this highlights, with the correct user-centred tools, that domestic users are able to gain new insight into their networks to support self-management.

### **1.3 Automating user-centred presentations of network data**

The work undertaken to address user-centred presentations of network data found that the annotation process places a significant time burden on users. Despite the benefits of HomeNetViewer, this issue limits its utility. To address this an exploration of applying enterprise traffic classification to automate the annotation process is undertaken. The question this section addresses is:

**Q4.0** Can enterprise traffic classification techniques be used with user contributed annotations to automatically annotate domestic network traffic?

A review of the current enterprise traffic classification literature is undertaken to highlight current practice in this area. Then the highlighted techniques are

---

tested agents the HomeNetViewer dataset generated in the HomeNetViewer deployment described in Chapter 4.

The outcome of this chapter is that current enterprise traffic classification techniques struggle to classify the data annotated by HomeNetViewer, for several reasons. It concludes by suggesting two ways in which these difficulties could be addressed in future work. The next section outlines the structure of the dissertation.

## 1.4 Thesis structure

The three strands of this dissertation explore different issues affecting domestic network usability. However, they share a common user-centred approach. They focus on how the domestic network infrastructure should be modified to better support self-management by users. They consider where the user should be included in the process and what is the most appropriate form of the interaction, within a domestic setting, to support the users' goals.

Chapter 2 presents the related work in four main sections. First, the academic work supporting the assertion that domestic networks need to be reinvented is provided, before exploring the literature on domestic network usability problems. Second, a detailed review of secure device association is presented to support the work on reinventing Wi-Fi device association, in Chapter 3. Third, the literature addressing domestic network legibility to support the work contained in Chapter 4 is reviewed. Finally, enterprise traffic classification is covered to support the work in Chapter 5.

Chapter 3 presents the work undertaken to address Wi-Fi device association, Chapter 4 covers the work relating to domestic network legibility and Chapter 5 explores enterprise traffic classification in domestic environments. The final chapter draws together the key lessons learned and open questions from Chapters 3, 4 and 5.

# Chapter 2

## Background

This chapter overviews the existing literature pertaining to domestic networks and their users. First, an overview of the current technical implementation of domestic network infrastructure is given. Then discussion of the context and challenges of domestic networks is presented alongside literature pertaining to them. Following on from this, a detailed review of the literature related to Wi-Fi device association and enterprise traffic classification is presented to support the work in this thesis.

### 2.1 Domestic networks

Domestic networks are now common place and have become an unremarkable feature of everyday life [24]. These networks are used to access a vast array of content and services on a daily basis. Despite their widespread deployment the management, configuration, and control of this domestic resource imposes a significant technical burden their users [13, 29, 79]. This dissertation explores a user-centred approach to redesigning the domestic network infrastructure to address these issues.

**Domestic networking technologies** are not currently specifically standardised. Instead, current deployments are constructed using a number of recognised standards. Each manufacturer is free to chose the standards they implement. Thankfully, for the sake of compatibility with the wider Internet, most domestic

---

networking technology commercially available are based on the Internet protocol suite.

The Internet protocol suite is published by Institute of Electrical and Electronics Engineers (IEEE). It is fundamentally concerned with how data is transmitted over a physical medium from one system to another over a network. Hence it is the foundation of many different types of network, including domestic networks. Networks also require a number of other protocols to operate effectively. These are built on top of the Internet protocol suite. These protocols are standardised by the Internet Engineering Task Force (IETF), whose mission is “to make the Internet work better”. Standards developed by both the IEEE and IETF are commonly used in domestic networks and are described in more detail below.

The Internet protocol suite is constructed using a layered approach. Each layer provides a specific set of functionality that is exposed to the layers above and below. Each layer operates independently of other layers. This maximises the flexibility and minimises the complexity for developers and network engineers [33].

The Internet protocol suite is built using four layers: link layer, Internet layer, Transport layer and Application layer. Each layer can be implemented using a number of protocols depending on the required properties of the network being constructed. Domestic networks use a common set of protocols at each layer. The function of each layer, and the common protocols used in domestic networks are described next. The Internet protocol runs on top of a fifth layer, the physical layer.

The physical layer describes the basic network hardware required to construct a network. It specifies the means of transmitting raw bits from one over a physical link connecting two nodes. The physical layer provides the functionality required to communicate directly between two nodes directly connected by a physical link. Many different types of physical layer technologies are deployed in the wider Internet. However, only three are commonly used in domestic networking. These are: IEEE 802.3 Ethernet, and its newer variants [3], IEEE 802.11 Wireless LANs [4], and IEEE 1901 Standard for Broadband over Power Line Networks [2].

Wireless LANs are implemented using radio frequency technologies, which are easily intercepted as they penetrate physical boundaries. To overcome this security limitation, communications over Wireless LANs are often encrypted using

---

Wi-Fi Protected Access 2 (WPA2). WPA2 is standardised in IEEE 802.11i-2004 [1]. WPA2 is now the standard protocol of choice for Wi-Fi security in domestic environments. Many domestic access points also support Wi-Fi Protected Setup (WPS), that is designed to address the complexities of configuring WPA2 enabled devices. WPS, created by the Wi-Fi Alliance <sup>1</sup> and introduced in 2006, is discussed in more detail in Section 2.5.

The Internet layer is commonly provided by the Internet Protocol version 4 (IPv4). IPv4 specifies best effort end-to-end communication over packet switched networks. IPv4 was created to route traffic over the Internet. The current implementation of IPv4 is described in RFC791 and was first published in 1981 [71]. RFC791 is specifically limited in scope and deals with the fundamental functions necessary to deliver data from one host to another over an interconnected system of networks. IPv4 provides detailed information on host addressing, packet format/structure and packet fragmentation and reassembly. The roll-out of Internet Protocol version 6 (IPv6) in domestic environments has not begun. However it may be deployed in future.

The Transport layer is implemented using two main protocols in domestic, corporate, and backbone networks. These are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP was first described in 1974 [19] and later standardised, September 1981 in RFC793 [72]. It provides a connection orientated, end-to-end, reliable, in order communication channel between pairs of processes running on host computers attached to interconnected networks. UDP is a simpler protocol, standardised in RFC768 [70]. It provides a connectionless, end-to-end communication between pairs of processes attached to interconnected networks, but makes no guarantee that the data will arrive or that it will arrive in order.

The application layer encapsulates the high-level communications protocols used in process-to-process communications over a network. Many of today's application protocols are built on top of UDP. Two such protocols that are fundamental to the operation of domestic networks are Dynamic Host Configuration Protocol (DHCP) [28] and Domain Name System (DNS) [59]. DHCP provides a framework for passing configuration information to hosts on a IP network. It

---

<sup>1</sup><http://www.wi-fi.org/>

---

enables the automatic configuration of IP addresses and other configuration information to boot strap devices onto an IP network. DNS is a protocol and service that is used to translate human-readable domain names into machine-readable IP addresses. Protocols built on top of TCP are used where more reliable communication is required, such as, HTTP and HTTPS.

Each layer requires careful configuration, as misconfiguration at any layer can cause poor performance or broken connectivity. In domestic environments some of this configuration is performed upfront by the router designers. They select the appropriate parts of the network stack, and set sensible defaults for the many configuration parameters, for example choosing the internal IP range for the network. Domestic access points make many of these settings editable through a web interface delivered over the local network. This upfront configuration shields the domestic user from many of these complexities as long as everything is working correctly.

However, domestic networks are dynamic: new devices are added, new software installed, and operating systems are updated. When changes are made or things go wrong, the user is required to interact with the networking infrastructure. At these points of interaction, the user is often confronted with complex interfaces filled with technical terminology. Recent usability studies into the major brands of domestic networking devices show that they “use a complex, feature-oriented, rudimentary user interface (UI) design with terms that are understood by a very small percentage of people” [58].

Domestic networks are built using a host of protocols, tools, and technologies described above. They are designed for use on the wider Internet and enterprise networks to enable efficient, secure, and reliable access to the wider Internet. These technologies are complex and time consuming to deploy, and often require expert knowledge to configure. The complexity and technical focus of domestic networking infrastructure is a barrier to adoption for domestic users and are the cause of many usability problems. Next, a discussion of the domestic user is presented, paying attention to the differences between them and enterprise users.

---

## 2.2 The domestic context of networks

The domestic context is complex, and has many facets that make it an interesting diverse environment to study. Understanding the domestic context is key to properly applying a user-centred design approach. The domestic context is made up of the: domestic users, a home, and the technology used by its occupants.

The evolution of modern digital content and services has significantly changed the role of domestic networks in recent times. Domestic networks are built using the same protocols and tools that were developed for the Internet as a whole. While these have proven to be flexible, they were designed with a certain set of assumptions for a particular context-of-use: assuming trustworthy hosts, trained network administrators, and scalability to millions of nodes. This section looks at domestic users, the domestic environment and how they interact with networking technologies deployed within them. The first step required to apply user-centred design is to understand the users' goals and behaviours, alongside the context-of-use.

**The domestic user:** Domestic users are usually not trained networking professionals [30]. This means that domestic networks are predominantly self managed by non-expert users who have little interest in networking technology. This is supported by the findings of Grinter et al. who find that users are unable to verbally articulate information about their networks [38]. To make matters worse only a small percentage of domestic users understand the complex terminology used in network infrastructure interfaces and tools [58]. The mismatch between the assumption that networks will be managed by trained networking professionals and the knowledge of domestic users, contributes to many of the usability problems that are found in domestic networks.

Domestic users also have different goals to enterprise users. Domestic users do not have a shared goal, to produce a product or deliver a service, as is the case for enterprise users. Instead they have a diverse range of disparate concerns [25].

Poole et al. find that domestic users think differently about networks to networking experts [68]. They used householder-created sketch network diagrams to assess how people visualised their network infrastructure. This is supported



---

by the field work undertaken by Brundell in [18]. They find that domestic users reason about their network in teams of activities, applications, and users rather than IP addresses, ports, and protocols of networking professionals.

These factors combined make designing for domestic users different to designing for enterprise users. However, understanding the user is only part of the problem. To fully explore the domestic networking infrastructure the context into which it is deployed must also be taken into consideration. This is discussed next.

**The domestic context:** Domestic networks are somewhat different to enterprise networks: they have a small number of nodes, are predominantly self managed by non-expert users and contain a variety of devices from PCs to fridges. Domestic networks are also situated in the domestic context. These are rich diverse and dynamic social environments. O’Brien and Rodden explore the role of interactive domestic technologies in domestic environments and argue that there is a distinction between designing technologies for the home and for work [65]. They highlight four areas that impact the design of interactive technologies for the home: daily routine, ownership of space, coordination of home life and management of ‘overloaded space’.

Poole et al. also come to similar conclusions when they specifically studied domestic networks [68]. They suggest three areas where current networking infrastructure needs to improve to support self-management by users. Firstly, designing for time as the evolving nature of the domestic network require the design of tools that can archive the state of the network to enable changes to be tracked. Second, designing for space. The physical arrangement of devices in the home has a meaning to its occupants, and impacts the usage and policies for a particular device. For example, some parents would like to restrict access to the Internet in the children’s bedrooms. Finally, designing for household routines. The social aspects of the household often affect the operation of the domestic network infrastructure.

This work highlights the subtle interplay between the routines, practices, and arrangement of physical space in the domestic environment with networking technology. This interaction between technology and the social aspects of domestic

---

environments has been explored by a number of researchers focusing on domestic networks. Their work is discussed next.

**Socio-technical aspects of domestic networks:** Empirical studies by Grinter et al. revealed that domestic networks are characterised by “coordination challenges” [38]. For example, troubleshooting, network administration, configuration and management of shared resources all require coordinated action. Furthermore, the domestic network is influenced by the relationships and power structures within the household, Occupants create locally negotiated norms and expected behaviours of network usage and the devices connected to it [88].

This “local negotiation” or “collaborative management” between occupants is further explored by Crabtree et. al. who studied a comic-book style interface for domestic network policy creation and configuration [26]. Their results suggest “network policy in domestic contexts ... are shaped by and answerable to the moral reasoning that governs domestic life.”.

Crabtree et. al. also highlight three properties of domestic network policy making: network rules are about people, network rules are socially situated and network rules are open to interpretation and renegotiation. These make formal specification and automatic enforcement of domestic network policy undesirable. These findings have significant implications for the design of domestic network policy systems. Crabtree et. al. provide two important reflections on their work that directly influence this thesis.

*Network policy lives in the home not the network.* Domestic network policy are framed in the wider social context of the domestic environment. They are understandings and agreements that are processed in the social context and renegotiated as necessary. In contrast, enterprise network policy is predominantly about the network itself and the things attached to it. Enterprise network policy is often formally specified and evolves slowly with the changing need of the enterprise. The flexibility of domestic network policy makes systems that try to enforce them impractical.

*Many policies will remain unwritten.* Rules do not require formal specification for their use. In these cases Crabtree et. al. suggest, “it is more useful to convey awareness of network activities that are relevant to rule use, enabling

---

members to surreptitiously monitor what is happening in the environment and take appropriate action.” [26]. This approach recognises the limitation of the technology to understand the rapidly adapting domestic context. Instead it focuses on supporting users by improving their situational awareness enabling them to take informed action as they see fit.

## 2.3 Domestic network challenges

Many domestic network users have to perform tasks that would not look out of place in large corporate networks, such as configuration of routers, cabling, backups, troubleshooting and fault resolution. In ‘Home networking and HCI: what hath god wrought?’ Shehan and Edwards discuss some of the complexities of the home network stating six factors that combine to create complexity [79]. These are:

1. Multiplicity and complexity of the devices.
2. The need to coordinate with outside agencies.
3. The division of labour.
4. The lack of planning.
5. The need for security configuration.
6. The invisibility of the infrastructure.

The impact of each is discussed in turn below.

**Multiplicity and complexity of the devices** . Domestic networks must support a bewildering array of devices, from PCs and mobile phones, to fridges and thermostats. These devices have different purposes and are often designed by different manufacturers. Each device has its own set of hardware and software that must be compatible with the network to function. Devices often require configuration to function correctly, and each offers its own interface to accomplish this task. These interfaces are individually designed and are often inconsistent

---

between devices from different manufacturers. Each device also has its own interaction affordances. Some provide screens and keyboards, while others provide just a few buttons. These factors combine to create a confusing set of interactions to achieve even the simplest task, for example, adding a new device to the network [42].

**The need to coordinate with outside agencies** . The domestic network does not operate in isolation. It must connect to the wider Internet to fulfil its role. This requires coordination with outside agencies, such as Internet service providers. This issue complicates fault diagnosis with users often unsure whether the fault is with their network, the Internet service provider, or the wider Internet [85]. Poole et al. explore this issue further by looking at the interaction between domestic users and technical phone support staff [67]. They found that the technical properties of domestic networks and the physical structure of the home can complicate remote support of domestic networks.

**The division of labour** . Domestic networks are not jointly managed by all members of the household. Often a single person will take responsibility [38]. This person is often a family member, but could also be friends or neighbours who are called-upon to act as external support when the domestic network breaks. The prevalence of these “gurus” can be seen as evidence that domestic networks are not usable by a large section of the population [45, 69].

**The lack of planning** . Enterprise networks are carefully planned and managed to ensure smooth operation and flexible provisioning. Network planning and provisioning is a profession, undertaken by trained teams. In contrast, domestic network planning focuses on the location of new devices in the home, how not to break the existing network, and reducing disruption to household routines [37]. While these have a resemblance to the activities of enterprise network planning and provisioning they are fundamentally different. For example, new devices are added to domestic networks in an ad-hoc fashion, located based on aesthetics, and the arrangement of the domestic space.

---

**The need for security configuration** . Correctly securing a network is a challenge, even for trained professionals. Security threats come from a number of sources and are constantly evolving. Most domestic users are untrained and do not have the time to keep up-to-date with the latest security threats.

Furthermore, research into how untrained users handle security has shown that they avoid security related decisions, due to a lack of knowledge [93], and the belief that others, for example, banks, software companies, and Internet service providers will manage security on their behalf [27] . However, when they do make choices, most rely on incomplete mental models, that can lead to inaccurate decisions being made [93]. These factors have been associated with poor Wi-Fi security practices [42], and the spread of malware and viruses [93]. Various approaches have been explored in an attempt to address this, for example, outsourcing home network security [32].

**The invisibility of the infrastructure** . Edwards et al. define infrastructure as:

“a broad term that can be applied to any system, organizational structure, or physical facility that supports an organization or society in general; this broad term has been used to describe interconnect systems that sink into the background of everyday life (e.g., roads, sewers, or telecommunications networks)” [31]

The domestic network infrastructure supports us in our everyday lives and is often practically invisible to the end user, never revealing its true complexity. This invisibility leads to complacency on the part of the user, and an expectation that the system will “just work”. For example, the last time you turned on the tap did you consider the vast network of pipes, pumps and treatment plants that allow clean water to be delivered to your home?

The invisibility of the infrastructure and the fact that it mostly “just works”, breeds complacency amongst users. This complacency causes poor documentation of the systems already deployed [31]. This, combined with the division of labour, makes trouble shooting, adding new devices, and changing the configuration to enable new services, a daunting task for most users.

---

This poor understanding is brought to the forefront when the infrastructure fails. Only then does the complexity of the system reveal itself. It is at this point the users realise they do not have the knowledge to fix it themselves. This is all too evident in the home network, when that important email must be sent, but for some reason all the users gets is an incomprehensible error message. This lack of expert knowledge is only part of the problem.

Another place where the invisibility of the infrastructure impacts on the usability of the domestic network infrastructure is in network policy creation and enforcement. Domestic network policy enterprise policies are prospective, designed to stop a defined set of undesirable actions. Domestic network policies are retrospective and situated within the moral ordering of domestic life [26]. Furthermore, the domestic network is influenced by the relationships of the occupants within the household, who create locally negotiated norms and expected behaviours around network usage and the use of devices connected to it [89]. Enforcing locally negotiated rules requires an understanding of the network infrastructure and what is happening on it. However, currently available domestic networking tools do not support this hindering the process [38, 88]. This is referred to as the Legibility problem.

The next section explores the current thinking on how best to address usability problems within domestic networks.

## 2.4 Addressing the challenges

The empirical studies discussed above show that currently deployed domestic networks do not fit the domestic context. This mismatch between the technology and the social aspects of domestic environments leads too many of its usability problems. Early attempts at addressing this problem focused on technical solutions. New protocols like Simple Service Discovery (SSDP) used by UPnP [56], and Zeroconf [83] were developed. These focus on making the configuration process automatic, without user involvement. UPnP and ZeroConf only address a limited subset of domestic network configuration problems [95], and have been criticised for weakening network security [39].

---

Recently a new direction has emerged, which focuses on addressing the invisibility of the infrastructure, sometimes called the infrastructure problem. Edwards et al. highlight three facets of the infrastructure problem [31]. First, *constrained possibilities* that they define as design choices in the infrastructure that may constrain desirable user experience outcomes. Second, *interjected abstractions*, where complex aspects of the technical implementation are present in the user interface. Finally, *un-mediated interaction* where physical interaction with the infrastructure is required to achieve the users' goal. They argue that these three emergent properties of current domestic networking infrastructure hinder the creation of more user friendly domestic networks.

The constrained possibilities highlighted by Edwards et al. have led the HCI community to rethink how and where HCI practitioners should be involved in the design of the domestic network infrastructure. Edwards suggests that the HCI community needs to be involved provocatively with the creation of the technical infrastructure supporting domestic networks [31].

Recently some members of the HCI community have started to explore how and where the infrastructure can be augmented to improve usability. Sventek et al. have created a new router platform (Homework) that includes an “information plane” [86]. The information plane they describe collects data on the operation of the router and the traffic going through it, for example, DHCP leases, IP Flows and RSSI information. The primary goal of the information plane is to collect and store network activity to enable a variety of new systems and services to be explored in the home.

Mortier et al. build on top of the Homework platform and explore putting user interaction into the infrastructure [63]. They explore two strategies. First, putting people in the protocol, which they illustrate through the modification of the DHCP protocol to require user interaction to confirm the device requesting an IP address is allowed to access the network. Second, bringing services closer to users, which they demonstrate by modifying the DNS protocol to allow or deny name resolution for particular sites for particular devices. A calendar based interface was then created to leverage this new functionality. This platform was then deployed in 12 households for a three month period. The “in the wild” deployment led to four observations:

- 
- **The invisible nature of a mundane infrastructure.** Over time the systems passive displays became just another part of the invisible infrastructure, ignored by the users unless a specific need arose or notification was raised.
  - **Increasing network information increases social discord.** Increased visibility of network activity caused several tense conversations around bandwidth sharing.
  - **The challenge of privacy.** Making previously hidden network activity available in an archive accessible through the system exposes new possible sensitive data to the rest of the household.
  - **Managing the network is managing the household.** New functionalities added to the system related to controlling or limiting access to the network have social implications and are subject to domestic judgements. What activity is most important and who has access is all related to the relationships between the occupants.

The work of Sventek and Mortier shows that by altering the underlying domestic network infrastructure, the creation of interesting new features that are of benefit to domestic users is possible.

It is upon the work above that this dissertation wishes to build. This work takes a user-centred approach to redesigning domestic network infrastructure to create user-centred solutions specifically for domestic networks. It can be seen from Section 2.3 that there are many problems. Addressing them all would be impractical. Therefore, two will be selected to explore in detail.

The first challenge explored is the simple act of adding devices to a Wi-Fi network, more formally known as secure device association. This is an act of securely introducing a new device to another device, over a wireless communication medium, without access to a public key infrastructure or trusted third party. In the case of domestic networking, this could be the addition of a new device to an existing wireless access point. This security-critical interaction with the infrastructure has been shown to be a point of frustration for domestic network users [42].



---

The second problem addressed is the legibility problem. This has been highlighted by recent observational studies of domestic networks. A number of socio-technical strategies for management and control of domestic networks have been observed “in the wild” [24]. However, this type of socially mediated network policy is not well supported by currently deployed domestic networking infrastructure.

These two challenges have been explored to varying degrees in the academic literature. The next two sections explore these problems and the related academic work in more detail. First, secure device association is reviewed before moving on to domestic network legibility.

## 2.5 Wi-Fi device association

To explore the issues related to Wi-Fi device association an overview of currently deployed technologies is presented before looking at the academic research. There are several currently deployed methods for securely associating a Wi-Fi device to a Wi-Fi network. Wi-Fi security is described in the 802.11i standard commonly called WPA2 [4]. Several older standards exist and have been superseded by WPA2 recently. WPA2 supports several methods of Wi-Fi device association that have gained widespread adoption in consumer access points. These are described in the following paragraphs.

**Manual passphrase entry** is the most commonly used method of associating a new devices to a Wi-Fi network, and is implemented by most devices as a fall-back from other methods. The system takes advantage of a shared secret that the user associating a device to the network must know. In the case of WPA2 this takes the form of an alphanumeric passphrase (formally, the Pairwise Master Key, PMK) combined with the network name (formally, the Service Set Identifier, SSID): if the user knows both, then they can add the device to the network. The SSID is usually broadcast in the clear, with most devices allowing the user to select it from a list. The network’s passphrase is often preconfigured and printed on the bottom of the Access Point (AP) or chosen by the user when they initially configure the AP. When the user provides the SSID and passphrase, the Ex-

---

tensible Authentication Protocol exchange sets up an encrypted communication channel between the device and AP.

**Wi-Fi protected setup (WPS)** is a standard from the Wi-Fi Alliance addressing usability issues with manual configuration of Wi-Fi networks [5]. It offers users a standard way to setup security protected Wi-Fi networks, removing the need for manual configuration. WPS offers three methods of configuration. First, in-band configuration that requires users to begin the pairing process by manually entering a 4 or 8 digit PIN into the device being added. This method requires only knowledge of the PIN and the device to be in range of the AP to enable successful pairing. The PIN can be static (printed on the AP and used for all association attempts) or temporary (used once per association attempt). Second, Out-of-Band (OOB) configuration that uses RFID or NFC tokens to pass keys between the device and the network. This method is not yet implemented in consumer hardware, and so it is not described further. Finally, push button configuration (PBC) provides a simple method to enable unauthenticated key exchange between the device and the network. The user starts the process by conditioning the device (various methods are used, but commonly they simply select the desired network from a list) and then conditioning the AP by pushing the WPS button. The AP will listen for a connection attempt for 120 seconds before timing out. If the connection attempt is successful Diffie-Hellman key exchange is used to create an encrypted channel over which the passphrase is exchanged, enabling subsequent communication to be encrypted via normal methods [57].

Unfortunately there are several problems with the currently deployed methods. The multiple step, many device, acronym filled setup experience involved in configuring a secure Wi-Fi network has been suggested as the root cause of many inexperienced users leaving their networks partially or completely unsecured. Ho and Dearman suggest, this is either due to lack of user understanding or simply the burden of the complex interaction [42].

Issues of passphrase memorability, confusion, incorrect recall and input error also affect the usability of manual passphrase entry that can be frustrating for users [75]. Manual passphrase entry methods are further complicated in domestic environments by the limited interaction capabilities of, and inconsistent implementation between, devices.

---

There are also considerable problems with WPS. Current implementations of in-band WPS are vulnerable to brute force attacks on the PIN [91]. Also, push button methods rely on physical access to both the device and the AP that can pose problems if either the device is not very mobile (e.g., a TV or refrigerator) or, as is increasingly common, the AP is hidden away and not easily accessible.

The problems with currently deployed device association methods highlights several areas where these technologies are a poor fit for domestic environments. First, the heterogeneity of the devices deployed in the home leads to an inconsistent implementation of the protocols. Second, the currently deployed protocols do not take into account the physical arrangement of domestic network, causing frustration. It is these challenges that this dissertation addresses. This is not the first work to present a solution to securely associating devices with domestic networks. Next, a review of device pairing mechanisms studied by the academic community is presented.

Academic research into securely associating a device with a home network is a particular case of the general problem of securely pairing two devices. This has been extensively studied by the usable security (HCIsec) community. It was first addressed by the “Resurrecting Duckling” protocol [82] which suggests that devices should be connected by a physical connection such as a cable for the pairing process to occur. “Talking to strangers” [8] takes a similar approach, but uses an infrared connection as the out-of-band channel to transfer credentials between devices. Both need little user involvement, but do require that the devices have a compatible hardware interface, which is often not the case in today’s complex device ecosystem.

Numerous other projects have approached this problem through the use of out-of-band channels and user involvement. “Seeing is believing” (SiB) [55] introduces visual out-of-band channels for mutual authentication of two camera-equipped wireless devices, using 2D barcodes to explore the general problem of bootstrapping encrypted communication between mobile devices and access points. Blinking Lights [77] simplifies this to requiring only a unidirectional visual out-of-band channel to mutually authenticate devices. A single flashing LED on one device and the camera on the second device enable transfer of the short authentication code. Shake Well Before Use, attempts to address secure device

---

pairing for devices with limited input capability, using a novel interaction where both devices are shaken together by the user to generate a shared secret for the establishment of a secure wireless connection [54].

“Network-in-a-Box: How to Set Up a Secure Wireless Network in Under a Minute” [7] uses location-limited channels to perform the out-of-band key exchange in an attempt to address the usability issues of the pairing problem. These location-limited channels usually have lower bandwidth and higher latency than normal network communication mediums. Their implementation uses short-range infra-red to provide an intuitive point-to-authenticate gesture for out-of-band public key exchange, bootstrapping the wireless joining process. Similar approaches using different out-of-band channels have been suggested, such as, “Loud and clear” [34] and HAPADEP [81]: both use auditory channels for credential exchange. For a detailed review of other methods see [47, 49].

Each of these approaches reduces the burden on the user, but places considerable constraints on the hardware and/or software capabilities available on the AP and, worse, on the joining devices. For example, SiB and Blinking Lights require all devices to have a camera to read the network credentials, while Network-in-a-Box requires that devices and AP have an IR sender and receiver respectively. Such requirements are often impractical for low-cost single function devices like sensors and media streamers, due to the increased manufacturing costs. They can also rarely be met by the devices already deployed in the home, making backwards compatibility difficult to achieve. It is these practical limitations that have prevented adoption of the techniques suggested in the literature. However, there is a clear benefit to using OOB channels to reduce the burden on users streamlining the user interaction. Our work in this area attempts to exploit the benefits of OOB channels without imposing unrealistic hardware and software constraints and maintaining backwards compatibility.

## 2.6 Legibility of domestic networks

The challenge of network legibility is first highlighted by Brundell et al. in [18]. They point out that to support domestic users in the negotiation of network policy, users need to understand what is happening on their networks, and that

---

currently available networking tools do not provide this level of accountability and transparency. They also show a dichotomy between the enterprise and domestic views of network traffic.

Existing work on network data visualisation has shown that surfacing hidden data, such as bandwidth usage [20], can help the users develop a better understanding of the network. The visualisation of network data has also been shown to support negotiation of fair use of bandwidth. The body of work in this area so far has focused on the use of web interfaces and situated displays to engage the user with their data [95, 96], but is limited to displaying network configuration, devices connected and bandwidth usage. They provide little or no visibility on what is actually happening on the network, beyond device X is using 10% of the available bandwidth. While this information is useful for real time fault diagnosis it is far from comprehensive. No information is provided to enable users to see **what** a device is doing or **who** is doing it.

Domestic data annotation has generated some recent research interest in the field of domestic energy usage [22, 74]. Of particular interest is the recent work undertaken by Costanza et. al., as it has some similarities to our work [22]. Although the target data source is different, Costanza’s main goal is to “allow users to engage with and understand their energy consumption data”. This is achieved using an interactive visualisation of live and historical energy data with user contributed annotations. The goal was to help people link their **activities** to their energy consumption. In this work energy consumption visualised is through occupant activities rather than just appliance readings. There were three key findings. First, time-series historical visualisation provided much more information than the traditional instantaneous monitoring of devices. Second, interactive visualisation and annotation can help users relate complex data to their everyday lives through activities. Third, the link between activities and usage data helps people understand how their actions impact energy usage.

Bates and Broadbent have also presented a position paper that suggests combining network data and energy data with an annotation platform to better understand activities, users and energy usage [10].

Enterprise network traffic classification has many uses in accounting, planning, provisioning, quality of service, and detection of malicious activity. Consequently,

---

it has been the focus of a large body of research and has been shown to be a difficult task. This body of work has highlighted many challenges and presented a number of approaches to address them. This section will provide an overview of core network classification techniques with a view to how they might be applicable to the domestic environment.

Early attempts at traffic classification relied solely on the use of well known port numbers. These are managed by The Internet Assigned Numbers Authority (IANA) in the Service Name and Transport Protocol Port Number Registry [23]. Ports were assigned to applications on a first-come-first-served basis. Port numbers are between 0 and 65535 and are split into three distinct ranges: 0 to 1023 are system ports, 1024 to 49151 are user ports and 49152 to 65535 are the dynamic ports. The correct usage of these ranges has been specified [23]. Only the system ports and the user ports are registered with the IANA. The first network monitoring solutions relied on this set of agreed ports to determine the types of traffic passing through a network [61]. While this approach was successful for a while it eventually started to fail for two reasons. First, new protocols were encapsulated in other protocols, for example, HTTP. Second, use of port numbers is only a convention and cannot be enforced. Therefore, applications are often run “off port” to avoid firewall restrictions or to hide malicious activity. This problem was quantified by Moore and Papagiannaki [61]. They showed port based methods could only correctly classify 69% of application flows in their dataset. To address the limitation of port based approaches packet payload inspection or Deep Packet Inspection (DPI) techniques were developed.

DPI relies on the capture and analysis of the full IP packet and its payload. It provides greater accuracy and is available in a number of commercial applications e.g Ellacoya<sup>1</sup> and Packeteer<sup>2</sup>. However, it has a number of drawbacks. Firstly, it is very resource intensive and does not scale well to high bandwidth. Second, it is reliant on hand crafted application signatures to enable pattern matching within the payloads. Maintaining and creating these adds a significant staffing overhead. Finally, DPI is not effective if the traffic is encrypted. These drawbacks forced

---

<sup>1</sup><http://www.ellacoya.com>

<sup>2</sup><http://www.packeteer.com>

---

researchers to examine new techniques, namely, host behaviour and statistical fingerprinting.

Host behaviour based techniques examine the “social interaction” between hosts on the network, and look for tell-tale communication patterns. The first work to explore this area was Blinc [44]. They classified flows captured on several enterprise networks into eleven broad categories (web, p2p, data, Network management, mail, news, chat/irc, streaming, gaming, Non Payload and Unknown) with an accuracy of 80%-90%.

The limitations of port based methods, deep packet inspection and the requirement for greater accuracy led researchers to explore the use of statistical methods to classify network traffic. The use of Bayesian analysis or machine learning techniques was first proposed by Moore and Zues in 2005 [62]. Moore and Zues used a Naive Bayes classifier to assign traffic to ten classes: bulk, database, interactive, mail, services, www, P2P, attack, games and multimedia.

They used the properties available in the IP Flow records and IP packet headers as input data to their Bayesian classifier. IP flow records are defined as a tuple containing source IP address, destination IP address, source port, destination port, protocol number, duration, number of packets and bytes transferred. IP packets were grouped into flows using the IP five tuple as a unique key. The flows were then hand classified to provide ground truth for the learning algorithm. The applications (or protocols) were grouped into classes based on their “potential requirements from the network infrastructure” [62].

For these techniques to be effective in the domestic environment to overcome the lack transparency and accountability the classes must be of use to domestic users. The goal of this dissertation is to facilitate the local negotiation and monitoring of network policies, enabling self-management by users. These policies are often based around the user of a device performing particular activities [18]. Hence, the classification system should group traffic based around users and activities. User identification from network traffic has received much attention from a security and privacy perspective. Next, the academic literature relating to user identification is discussed before moving on to network activity recognition.

---

**User Identification using network data.** Our work aims to identify which user is using a device connected to the a domestic network within a household. This means the task is to identify a small set of users for whom a large amount of data is available. Hence, this is not a traditional identification problem where we need a single feature that is as close as possible, unique to a user, within a large population e.g. a fingerprint. What we are looking for are the characteristic patterns generated by user activity, which end hosts they visit, how often, and what are the properties of the generated flows. This behavioural approach has been examined by a number of authors concerned with the re-identification of users from various networking related data sources.

Herrmann et al. examine the feasibility of re-identifying users for a passive attacker monitoring DNS requests [41]. They use a dataset collected over two months containing the DNS records for more than 3600 users from the student living accommodation at their university. Herrmann et al. make an assumption that a single IP address in the dataset is linked to one user, which is valid as each user is assigned a static IP for their room. However, they note that there will be some noise present in the data due to students visiting friends and using a device they do not own. They build profiles for each user over a 24 hour period and test several classifiers and filtering techniques (sub-linear transform, normalisation, inverse document frequency).

Their best reported classifier is able to re-identify 85.4% of DNS requests to users. Herrmann also discusses the effects of some of the parameters in the model. Firstly, they show that the length of time the profile is built over has a significant impact on accuracy with longer time windows provided better accuracy. Second, they also notice the presence of a large number of DNS queries related to non-human activity (various checkers, software updates, e.t.c) in their dataset. Herrmann made an effort to manually filter out non-human activity and found it reduced the accuracy of their best classifier to 79.5%. This suggests that the behaviour of the host is an important source of noise in the of task of identifying users identification.

Another related body of work on user identification can be found in the data mining and information retrieval communities, where users are profiled from the data in web server log files, to enable personalisation and fraud detection. In some



---

work in this area profiling is extended to enable behaviour based user identification from web server log data [97]. In his work Yang develop their own profiling method, that extracts many behaviour profiles per user, then selects the most distinct profiles to be used in the identification phase. Yang’s method achieves 62% to 87% accuracy depending on the number of training sessions for a web server with 100 concurrent users.

Flow based behavioural profiling has also been attempted in “User Profiling and Re-identification” [50]. Kumpovst and Matyvs focus on re-identifying users on a University network for three protocols (HTTP, HTTPS and SSH) using behaviour profiles generated from historical traffic logs. Their dataset is a full set of flow records collected from Masaryk University network, but they do not state how many users, hosts and flows they collected or the time period it covers. They use a section of their dataset as a training set and derive a “vector of source IP address behaviour” aggregated over a 1 month time window. The vector of source IP address behaviour is then compared using cosine similarity measure weighted using inverse document frequency to the new vector of source IP address behaviour generated from the second section of the dataset. They report false positive rates of 67.9%, 59.8% and 21.3% for HTTP, HTTPS and SSH traffic respectively, giving true positive rates of 32.1%, 40.2% and 78.7%. There is no mention of how the authors linked the hosts to users, there seems to be an explicit assumption that a single host is only ever used by a single user and that hosts never change IP address. These may be valid assumptions for their dataset. However, they do not necessarily hold for domestic networks.

Now that we have reviewed the related literature the next chapter presents an exploration of user-centred mechanisms for infrastructure control. It begins by presenting the design of MultiNet, a system for Wi-Fi device association in domestic environments, before moving on to its evaluation, in terms of its performance and usability.

## Chapter 3

# User-centred mechanisms for domestic network infrastructure control

This chapter focuses on improving domestic network infrastructure control, in particular the task of Wi-Fi device association. As outlined in the background (see Section 2.5) currently deployed methods for Wi-Fi device association are not fit for purpose in domestic environments. The current situation is likely to be worsened by the recent trend towards the Internet Of Things (IoT), where devices are normally single function, network connected, with limited interaction capabilities.

To address the issues surrounding Wi-Fi device association, a user-centred design approach is adopted to create a user-centred mechanism for Wi-Fi device association designed specifically for domestic environments, called MultiNet. MultiNet provides a lightweight consistent interaction to securely associate devices with domestic wireless networks.

MultiNet is designed focusing on the needs of domestic users and the affordances of the domestic environment. MultiNet is used to explore the trade off between usability and performance in a domestic setting. Its design deliberately compromises network performance to improve the user experience. MultiNet substantially changes the device association process by inverting the credential

---

flow and creating one Wi-Fi network per device. Instead of configuring each device to one pre-configured network. MultiNet also takes advantage of an Out-of-Band communication channel, implemented using a third device, the *Network Controller*.

Before the final design of MultiNet is described, the process used to create it is presented. Firstly, a list of design parameters is drawn from an analysis of the literature and the domestic context. Second, the design of MultiNet is presented, paying special attention to how the design principles have been adhered to. Finally, the results of a network performance and usability evaluation are presented to compare MultiNet to existing Wi-Fi device association methods and explore the trade off between usability and performance.

### 3.1 MultiNet design

The design parameters of MultiNet are drawn from an analysis of the domestic context, domestic users, and academic literature. This leads to ten design parameters, to which the new system should conform. The goal is to design an interactionally lightweight and secure device association mechanism for domestic environments.

From the literature four accepted usability problems with Wi-Fi device association are exposed. Firstly, passphrases are difficult to remember and enter on some interface constrained devices. Second, inconsistent implementation of association methods causes usability issues, due to the differing interaction styles for each device. Third, splitting the interaction between the device and the access point, as in WPS push-button, is problematic for devices located in different areas of the home. Finally, users often do not understand the security implications of their actions. For example, choosing weak passphrases or disabling WPA2 to support an old device. This is due to the complexity of the underlying infrastructure and complex security model, combined with the need for users to make important security related choices. From these issues five design parameters were drawn:

DP1 The transfer of credentials should be automatic.

---

DP2 The interaction should be consistent for all devices irrespective of its interactional capability.

DP3 The interaction should be located in a single location, at the device or the access point.

DP4 The security model should be simple, limiting attack vectors to ones which users understand.

DP5 The security related choices should be minimised.

From the HCIsec literature we can see that there are clear benefits in using location limited out-of-band communication channels for credential transfer. However, out-of-band communication channels place unrealistic constraints on the devices and infrastructure. This leads to the following design principle.

DP6 The interaction should not require that devices have particular hardware to perform credential exchange.

From the literature concerning the socio-technical aspects of domestic networks a number of factors that affect our design choices are found. Domestic networks are usually built in an ad-hoc fashion, with new devices added from many manufacturers to perform a variety of functions. This piecemeal construction means that it is unlikely that a user will replace all their devices at the same time. Therefore, backwards compatibility with existing devices must be preserved. Current Wi-Fi association methods provide poor support for access revocation. Access revocation is important in domestic environments in a number of scenarios, for example, visitation or sale of a device. From these the following three design parameters are drawn.

DP7 Modification of the software on existing devices is not possible.

DP8 Modification of the hardware on existing devices is not possible.

DP9 Revocation of access should supported and have a lightweight interaction.

---

We also made a number of observations about how users manage security of the home more generally. Firstly, the home is a private space with access negotiated with the occupants. Second, the security of the items in the home is controlled by controlling physical access to private spaces using locked doors and cupboards, for example. The control of physical access and the securing of the boundaries of the home are common and well understood practices that people do automatically every day. This suggests the design parameter below.

DP10 The system should utilise the inherent physical security of the home and existing social conventions around access to the dwelling.

The next section describes the final implementation of MultiNet. Each piece of the system is discussed and the impact of the above design parameters is highlighted.

## 3.2 MultiNet implementation

MultiNet aims to address the usability issues of associating Wi-Fi devices in domestic environments. It has two key features which make it significantly different to current approaches. Firstly, the way in which the 802.11-2004 protocol is deployed is inverted. This means that the direction of credential transfer is reversed. Devices are preconfigured to associate with a specific network and the access point can be configured to offer this network enabling the device to connect, rather than configuring each device to a single network offered by the access point as is currently the case. This reversal creates one network per device, leading to multiple Wi-Fi networks, hence its name.

Second, an intermediary device, the *Network Controller* is introduced into the association process. The *Network Controller* acts as an interface to the network and provides the extra hardware required to perform credential exchange, over an out-of-band communication channel, between the access point and the device being associated, meeting DP1. The *Network Controller* allows the use of an out-of-band communication channel without placing hardware and software constraints on the devices joining the network, fulfilling DP6, DP7 and DP8. The

---

*Network Controller* also provides a single point of interaction with the network satisfying DP2 and DP3.

These two changes fundamentally alter the device association interaction and require modification of the underlying network infrastructure. Next, the modification required to implement MultiNet are discussed.

**Modifying the access point software.** The software running on the access point is modified to enable the creation of on-demand virtual access points for each device. Each virtual access point uses a different set of WPA2 credentials. These are provided by the device, through the *Network Controller*. An over view of MultiNet’s implementation is provided in Figure 3.1.

The *hostapd* user-space daemon is used to provide wireless access point and wireless authentication functionality conforming to the IEEE 802.11i WPA2 specification. *Hostapd* is mature open-source software and is commonly deployed in many commercial access point implementations. MultiNet requires that *Hostapd* is modified to enable dynamic creation and destruction of networks secured via the WPA2 protocol. The modifications made pre-allocate memory for state information, for example, WPA2 configuration and corresponding virtual network interfaces, for a maximum of 50 networks.

Upon creation of a new network, the associated virtual network interface is connected to a standard Linux layer 2 bridge (*br0*) to enable communication with other devices connected to the access point. The bridge interconnects all the per-device virtual networks, so IP traffic can propagate between all devices (the administration network for the *Network Controller* is excluded from the bridge to maintain isolation). Finally, the configuration re-load routines were modified to only de-authenticate stations when the SSID or passphrase of a network is changed or removed from the *hostapd* configuration file. The configuration file is re-read whenever *hostapd* receives a `SIGHUP`, issued each time a new virtual access point is configured or removed.

MultiNet exposes its new functionality to the *Network Controller* via a set of RESTful web services. These are only accessible over HTTPS using the WPA2-secured administrative network configured on the *Network Controller*. Each network created is presented as a distinct virtual interface joined to the global bridge

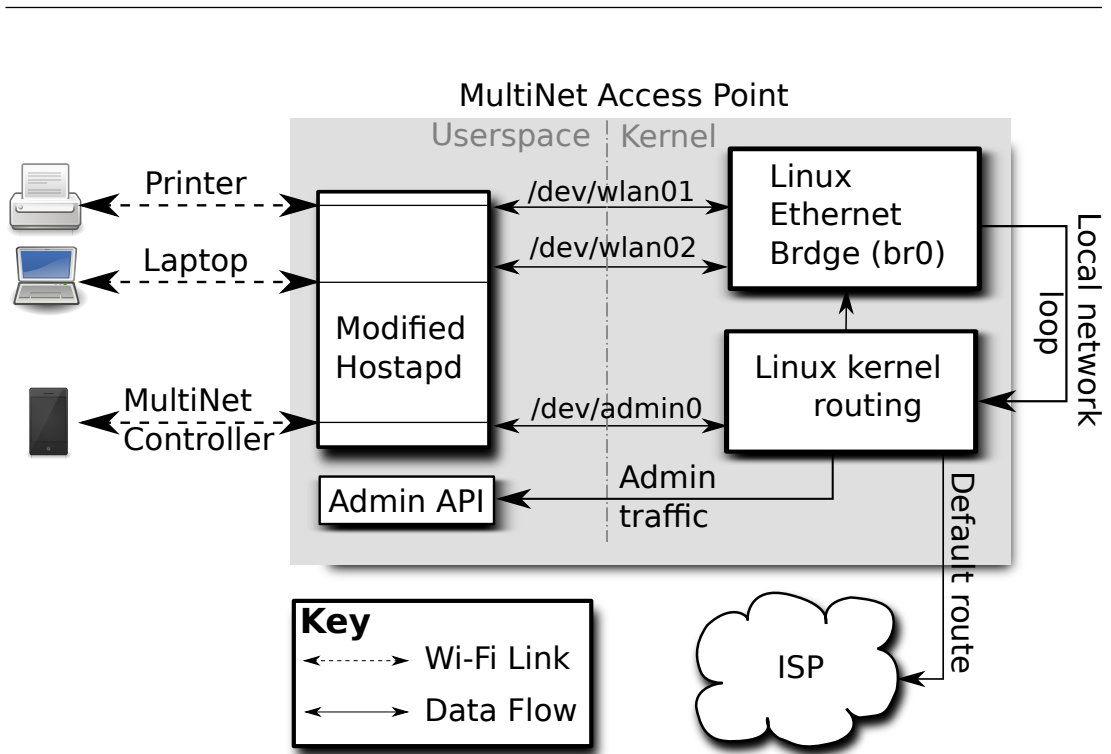


Figure 3.1: Overview of MultiNet implementation.

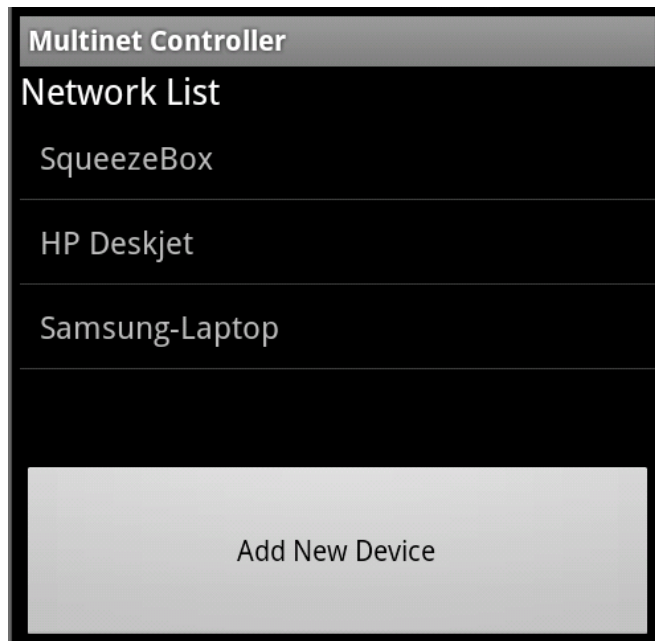


Figure 3.2: MultiNet *Network Controller* interface.

---

and routed to the outgoing upstream network interface. The *Network Controller's* administration network is not added to the bridge or routed upstream, isolating it. This protects administration functions from non-trusted devices connected to the access point. Consequently, the *Network Controller* only uses the administration network when the MultiNet configuration application is running. The normal network connectivity is provided by a standard device specific network.

**Implementing the Network Controller.** The *Network Controller* is connected to the access point via a dedicated WPA2-secured administrative network between the *Network Controller* and the access point. This arrangement enables a consistent configuration interaction to be used across all devices without imposing new hardware or software constraints, maintaining backwards compatibility with legacy equipment, fulfilling DP7 and DP8.

The current implementation of MultiNet uses a consumer smartphone as the *Network Controller*, with its built-in camera providing the visual out-of-band channel. The out-of-band channel is created using a QR Code affixed to the exterior of the associating device which has the required credentials for the WPA2 network encoded. Backwards compatibility requires *no* software or hardware modification. The device must simply be configured with an SSID and passphrase which are then affixed to its surface as a QR Code. The credentials can then be securely transmitted to the access point via the *Network Controller's* administration network. The access point then creates a virtual access point with the provided credentials and the new device can automatically associate to the new network. The overall protocol flow is depicted in Figure 3.3. The end result is that the access point provides many networks, roughly one per device.

The *Network Controller* is implemented as an application for an Android smartphone. When it is active, it attempts to join the administrative network. On success, it provides a list of active configured networks and a button to *add new device* to the network. The *Network Controller* provides feedback to the user when a device is added successfully. The interface shown in Figure 3.2 has been kept simple, intentionally, to avoid confusion. Credential exchange takes place over an out-of-band channel provided by the, *Network Controller*, and the hardware requirements for the out-of-band channel are abstracted to it. This



---

arrangement places no constraints on the hardware or software of the devices on the network beyond that already required, fulfilling DP7 and DP8.

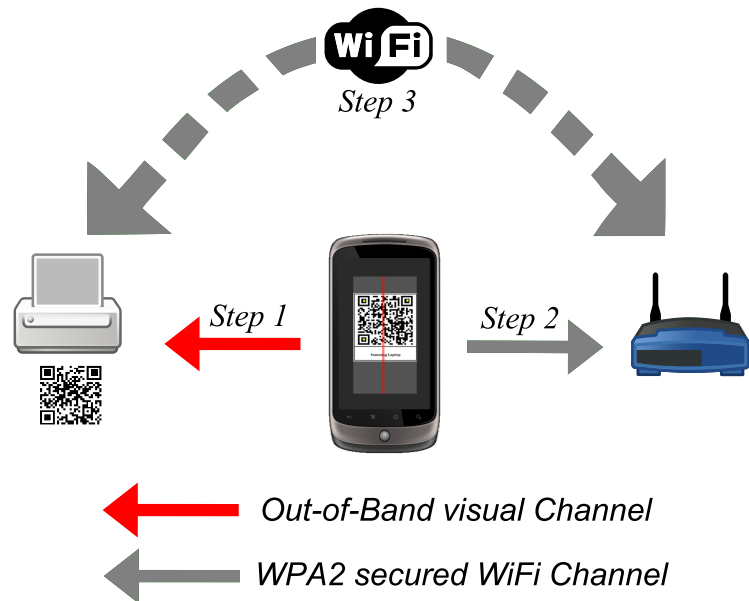
The *Network Controller* is a fundamental part of MultiNet. It provides several benefits in the device association process. Firstly, it moves the configuration task from the device being added, to the *Network Controller*. This overcomes the limited interaction capability of a number of devices found in the home, such as games consoles and smart fridges.

Second, the *Network Controller* itself can be an interactionally rich device with a touch screen, microphone, fingerprint sensor or camera, or whatever is required. This enables the creation of new otherwise impractical interactions for device association, which can be crafted to fit the needs of the domestic user. Third, it provides a centralised point of control for the network. Reducing the need for hard to find web interfaces. Fourth, the *Network Controller* is mobile. Its mobility enables the configuration to be carried out at the location where the device is being installed, which is important for large and/or distant devices. The interaction in WPS is often criticised for its dislocated interaction.

These four factors combined make it possible to build new interactions that take place in a single location, with a consistent interaction, which meets DP2 and DP3.

This implementation of MultiNet reuses a common smartphone. This device was chosen as they are widely available, have Wi-Fi and cameras, and can be re-purposed easily through the installation of Apps. However, the inclusion of a dedicated device for this purpose is also possible. For example, the router manufacturer could bundle a dedicated *Network Controller* pre-installed with the MultiNet software and pre-configured to use the administration network.

**Bootstrapping the Network Controller.** Before MultiNet can be used it is required that a *Network Controller* is securely associated with the administration network. This step is crucial as it establishes a trusted signalling channel over which other devices can be introduced. This only needs to be done once per *Network Controller*. Any WPA2 compliant device with a camera and the ability to install Apps can be used as the *Network Controller*. Most modern smartphones




---

*Step One* Use the camera on the *Network Controller* to read the QR Code on the device to be joined to the network.

---

*Step Two* Request that the device is joined to the network by sending the SSID/passphrase pair for the device's virtual network to the access point.

---

*Step Three* Establish the virtual network allowing the pre-configured device to join the network.

---

Figure 3.3: MultiNet interactions to add a device [16].

---

and tablets are a good fit for these criteria and they provide a low cost, convenient and incrementally deployable solution which is readily available in many homes.

The process of setting up the *Network Controller* is straightforward and has two steps. The access point is required to have two QR Codes affixed to its surface. One contains the install location of the *Network Controller* application. The other contains the credentials for the secure administrative network. Step one is to point a standard QR Code reader application running on the device the user wishes to use as the *Network Controller* at the first QR Code. This causes the user's device to be taken to a website where the controller application can be downloaded and installed just like any other application. Step two is to run the application and point the device's camera at the second QR Code containing the administration network credentials. The *Network Controller* application can then join the pre-configured administrative network on the router. This process securely associates the new *Network Controller* with the access point.

**Device Pre-Configuration.** MultiNet requires that devices are pre-configured with a unique SSID and passphrase. How this is achieved is an important question. Ideally, we envisage that all devices are pre-configured by the manufacturer before they are shipped to distributors. This would require minor changes to the manufacturing process as many devices already have serial numbers, MAC addresses and other information placed in their firmware at manufacture time. However, this is an unlikely scenario in the near future, as it would require large scale adoption before such changes would make commercial sense.

Thankfully, this is not the only option for pre-configuration of devices. MultiNet enables the configuration process for new devices to be outsourced. Outsourcing, where others (e.g, relatives, professionals or retailers) undertake the technical aspects of device management has been suggested in [68]. Device pre-configuration could easily be outsourced, resulting in a printed stick-on QR Code being affixed to the device at the time of purchase or by a professional network engineer. This approach negates the need for local configuration of network credentials.



Figure 3.4: Laptop client device with MultiNet QR Code encoded credentials.

**Credential Encoding.** Credentials are encoded in QR Codes that facilitate MultiNet’s simple scan and connect interaction mechanism. QR Codes were chosen for five main reasons. Firstly, they are easily machine readable, a fundamental requirement to remove the need to manually enter the configuration information. Second, they have a simple and fast point and capture interaction method that fits well with the goal of making the process quick and interactionally lightweight. Third, there is a degree of user familiarity with them, as they are commonly deployed in commercial situations. Fourth, they are resilient to wear and tear and have built in error correction. Finally, QR Codes can encode sufficient information for credential storage. They must be able to encode a unique credential (SSID and passphrase) for every networked device manufactured. The maximum length of an SSID is 25 bytes, and the maximum length WPA2 passphrase is 75 bytes, giving 100 bytes allowing ample credentials to be generated in combination. Figure 3.4 shows a MultiNet QR Code attached to a device in a suggested location.

**Adding Devices.** Associating a new device to the network is the primary goal of MultiNet and is straightforward, assuming the device being added has been per-

---

configured as described above. To add a new device the configuration application is opened on the *Network Controller* and the “add device” button is pressed. This activates the camera and starts scanning for QR codes. The *Network Controller* is then pointed at the QR Code on the new device. The *Network Controller* then decodes the QR Code and extracts the credentials. The credentials are then sent to the router over the administration network and are used to configure the virtual access point for the new device. At this point a new network has been created with the appropriate SSID and passphrase, and the *Network Controller* displays a success indication to the user. The new device will then associate with the newly created network as soon as networking is enabled. This process is shown in (Figure 3.3)

**Removing Devices.** From our analysis of the domestic context the removal of devices from the network was one feature that current systems cannot support easily. It is important in two domestic scenarios: providing temporary access to visitors and removing a device for resale or gifting. The *Network Controller* of MultiNet acts as a user interface to the network which makes this task relatively easy.

The *Network Controller* shows a list of configured devices that have networks configured as shown in Figure 3.2. Revoking access for a device is simple: a user simply selects the device from the list and chooses “remove”. The *Network Controller* then communicates with the MultiNet access point over the secure signalling channel, and the relevant network is removed.

Once the network has been removed the pre-configured device can no longer access its network using its stored credentials, effectively revoking its access to the network. This fully satisfies DP9. In the currently deployed system all devices share the same credentials, to remove a device it must be manually de-configured, or the network credentials must be changed and all remaining devices reconfigured. Both of these methods are hampered by the limited interaction capabilities of current devices.

**Compatibility With Existing Devices.** Backwards compatibility for legacy devices is crucial in domestic environments as many homes already have an ex-

---

tensive Wi-Fi deployment and home owners are unlikely to want to replace all their existing devices. Backwards compatibility is achieved by the home owner using the *Network Controller* to generate a QR Code with a unique SSID and passphrase. The legacy device can then be manually configured to this SSID and passphrase, and the generated QR Code printed out and affixed to it.

This process need only be done once per-device and once initial configuration is complete, the legacy device will behave the same as any other MultiNet-enabled device. This functionality enables new deployment and service models to be explored, allowing the creation of outsourced configuration models described by Shehan and Edwards [80]. Manufacturers, retail outlets and network professionals could offer new configuration services, generating and printing configurations, and affixing them to the device for later use by the device owner.

**Security considerations.** Users are known to have limited understanding of the security issues surrounding Wi-Fi networks [46]. MultiNet aims to simplify the security model through three aspects of its design: its use of a proximate out-of-band channel, its use of QR Codes for credential storage, and its use of per-device credentials (SSID and passphrase). We will deal with each in turn.

MultiNet uses a proximate out-of-band channel which provides three important benefits. Firstly, it removes the burden of managing and entering secure passphrases from the user and the devices. This allows the automatic generation of credentials, which can be longer and use a wider range of characters than those typically input manually due to mental and physical limitations. The generated passphrases thus increase the search space for brute force attacks making them impractical [87]. Using a proximate out-of-band channel in this way meets DP1 and DP5.

Second, Diffie-Hellman key exchange is no longer used to construct a secure signalling channel over an insecure medium. Diffie-Hellman is used in existing methods, for example, WPS and has been shown to be vulnerable to man-in-the-middle attacks [51]. Finally, at no point is the network left in an insecure open state. WPS PBC will allow any device to connect once the access point has been conditioned. The user has no control over which device eventually connects [52].

---

The use of QR Codes for credential storage has benefits and disadvantages. The first benefit is that reading a QR code requires line-of-sight, reasonable proximity, and the use of a camera to successfully capture a decodable image of the MultiNet credentials. Carrying out this type of attack covertly can be difficult and has a high chance of detection. For devices located within the home the difficulty of this type of attack is increased by the standard security routines of most homes, for example, locking doors and not allowing access to strangers. This physical interaction style was chosen to implement DP10.

For mobile devices which leave the safety of the home other strategies can be adopted to increase the physical security of the QR codes. For example: QR Codes could be removable for secure storage, privacy covers could be added requiring a flap to be lifted to expose the QR Code, or, on devices with screens, transient codes could be displayed on screen when a physical button is pressed or application is launched.

The proximate out-of-band channel implemented via QR codes creates an unambiguous threat model for the *Network Controller* and devices: *physical access is required*. This maps the wireless network's security onto the physical security of devices, something which users manage in their everyday lives. The physicality of the association interaction, increased passphrase entropy and the security routines of the household provide sufficient protection against collocated and remote attackers. MultiNet also has a number of other properties that are relevant to the security of domestic networks.

The many network design of MultiNet requires that each device has its own unique credentials. Per-device unique credentials enable temporary or permanent revocation of network access, which can be useful in a number of domestic scenarios. For instance, visitation, punitive control or when a device is sold, lost or stolen. Revoking access is simple and can be achieved by using the *Network Controller* to delete the relevant network. Re-associating revoked access is identical to the usual association procedure. In the case of loss, theft, or compromise of the *Network Controller* the access point must be reconfigured with credentials for a new administrative network, which must be printed and attached to the access point before configuring a new *Network Controller* using the bootstrapping procedure described earlier.

---

Finally, the lightweight interaction, in which the *Network Controller's* interface and device specific credentials enables the creation of new security policies, impractical or impossible with existing mechanisms. For example, revoking access after a set time period has elapsed, a period of absence, or a set number of connections has been made.

MultiNet has now been fully described and a discussion of its main features has been completed. The next section presents a lab based usability study of MultiNet before moving on to an analysis of how the modifications have affected the performance of the network.

### 3.3 MultiNet usability analysis

The primary objective of MultiNet is to improve the usability of domestic network device associations, without compromising security. To ascertain whether or not MultiNet provides enhanced usability over current methods, a comparative usability study was undertaken. The study compares MultiNet to WPS PBC, which was chosen for two reasons. Firstly, it is a standardised usability-focused device association method. Secondly, it is widely sported by consumer devices and has good market penetration [94]. The rest of this section describes the study in detail and presents the results obtained. The study was conducted in lab conditions with all participants performing the task of building a network using both WPS and MultiNet. Participants performed each task in the same lab with the same facilitator. Before the study a short pre-study survey was conducted to assess exposure to home networking, WPS and QR Codes. After the study was completed a post-study, semi-structured interview was used to capture participants' reactions to both systems.

#### 3.3.1 Participants

Sixteen participants took part in the study, ten male and six female. Participants were recruited from around the university campus using posters and mailing lists. Participants were given a £10 Amazon voucher to compensate them for the inconvenience of taking part in the study. Of the sixteen participants, ten indicated



---

	WPS	QR Codes
Never	12	6
Occasionally	1	8
Often	3	2

Table 3.1: Prior exposure to WPS and QR Codes.

Age Group	18–24	25–34	35–44	45–54	>54
Participants	4	9	0	2	1



Table 3.2: User trial participant age range.

they were the person responsible for configuring their own home network. However, only three of the participants were very confident they would be able to configure a new wireless-enabled device they had purchased. Twelve of the sixteen participants had never used WPS before and six had never used QR Codes. The networks of the participants were varied in size and complexity, with the number of connected devices ranging from 3 to 15 with a mean of 5.6 (SD = 3.8). Two of the sixteen participants were unable to provide detailed information on the devices and configuration of their home networks. Tables 3.1 and 3.2 give more details on the composition of the participants.


### 3.3.2 Method

The user trial consisted of a single task to construct a network consisting of three consumer devices. These were a HP Deskjet 3050A e-All-in-One Printer, a Squeezebox Radio and a Samsung laptop running Windows 7. The study had two conditions: C1, connecting the three devices using WPS PBC, and C2, connecting the three devices using MultiNet. The order in which the subjects experienced the two conditions was randomised to compensate for any carryover effect between conditions. In each condition the devices were identical and added to the network in the same order. We assumed that the MultiNet *Network Controller* had been previously bootstrapped to the network as this step would be carried out at network installation time, perhaps with the aid of the network service provider.

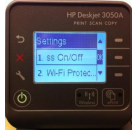
Participants received instructions on the use of the required features of the router before the task began in both conditions. Following the manufacturer’s

1.  To start the process press the Wireless button 

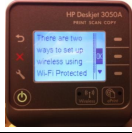
---

2.  Select 2. Wireless settings


---

3.  Select 2. Wi-Fi Protected Set Up (WPS)


---

4.  Select OK


---

5.  Select "Push Button" and follow the onscreen instructions.  
The device is connected when the blue Wi-Fi light stops flashing


(a) WPS

1.  Locate the device QR-code  
**Device Name**



---

2.  On the satellite controller select "add new device"

---

3. 
  - a) Align the QR-Code in the centre of the screen
  - b) Hold the satellite controller still for a few seconds.
  - c) A beep will sound and you will be returned to the main screen

---

4.  Turn the printer on using the power button 

---

5. The device is connected when the blue Wi-Fi light stops flashing

(b) MultiNet

Figure 3.5: Instructions for adding the printer to the network for WPS (top) and MultiNet (bottom).

---

instructions for adding the printer, it took an experienced systems' administrator over 10 minutes to achieve a successful connection via WPS. Although more concise, instructions for the other devices were still excessively complex. Thus, to ensure consistency in the level of guidance provided, we rewrote instructions for all devices in both conditions. Great care was taken to keep the level, style and amount of instruction consistent between the two conditions. See Figures 3.5a and 3.5b for examples of the instructions provided.

Immediately after experiencing each condition, participants were asked to complete a System Usability Scale (SUS) questionnaire to gather their opinions on the systems usability. The SUS [15] is a “quick'n'dirty” usability evaluation tool comprising 10 short Likert scale questions designed to quickly gather users' opinions on system usability (effectiveness, efficiency and satisfaction). It generates a score from 0 to 100, with higher scores indicating greater usability.

To compare both systems directly, we use *task completion time* as a measure of effectiveness, with lower times indicating greater effectiveness. We measured the time taken to complete each step in configuring the device as participants moved through the task under each condition. Timing started when the participant interacted with either the device or the instructions, and stopped when they had completed the last step in the configuration sequence. In the case of WPS we defined this as when the participant released the WPS button, successfully activating it. For MultiNet it was defined as the point the participant first turned on the device after successfully scanning the appropriate QR Code. These endpoints were chosen so the different connection times for the two methods did not affect the measured task times.

As well as task completion time we recorded whether the participant used the available instructions. Instructions were placed face down in front of each device and participants were asked to refer to them only if they felt they needed to. Instructions were recorded as having been used if a participant turned them over. After the participants had experienced both test conditions, a short semi-structured interview was conducted to understand their broader reactions. Each participant was asked the same questions and the answers were recorded for later analysis.

---

### 3.3.3 Results

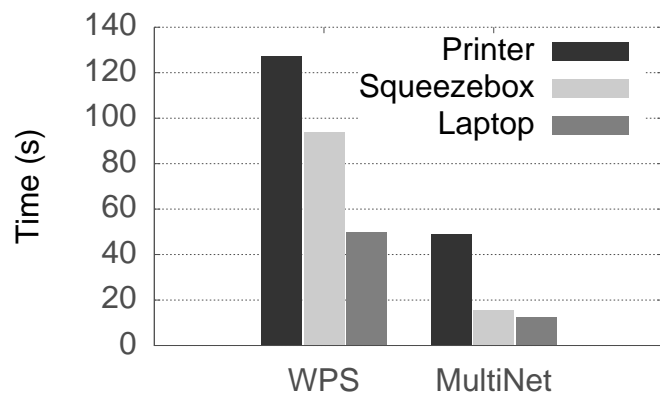
The mean SUS scores attained in our trial are WPS 81.88 ( $SD = 13.24$ ), and MultiNet 92.50 ( $SD = 11.03$ ). Empirical evaluation of large numbers of SUS scores across a range of products has shown that scores above 73 indicate good usability and score above 85 represent excellent usability [9]. The SUS scores thus indicate that both WPS and MultiNet are usable solutions, with MultiNet rated as more usable by the participants in our trial. A paired  $t$ -test on the SUS scores shows this difference in usability to be significant ( $t(15) = 5.36, p < 0.001$ ) with MultiNet having the higher mean score.

The mean task time measurements for connecting the printer using WPS and MultiNet were 127.56 seconds ( $SD = 69.23$ ) and 48.06 seconds ( $SD = 46.69$ ) respectively. A paired  $t$ -test shows a significant difference in task time for the printer of ( $t(15) = 5.65, p < 0.001$ ) with MultiNet having the lower times. For the Squeezebox Radio, the mean task time using WPS was 94.37 seconds ( $SD = 32.57$ ) and using MultiNet was 15.55 seconds ( $SD = 9.76$ ). Again, a paired  $t$ -test shows a significant difference in task times for the Squeezebox Radio of ( $t(15) = 10.29, p < 0.001$ ) with MultiNet having the lower times. Finally, connecting the Laptop using WPS gave a mean task time of 49.87 seconds ( $SD = 33.6$ ) while using MultiNet the mean task time was 12.26 seconds ( $SD = 5.23$ ). Once more, a paired  $t$ -test shows a significant difference in task time for the Laptop of ( $t(14) = 4.61, p < 0.001$ )<sup>1</sup> with MultiNet having the lower times. These results are summarised in Figure 3.6a. Analysing task completion time across all devices show that, using WPS the mean task time was 91.47 seconds ( $SD = 57.21$ ), while using MultiNet the mean task time was 25.92 seconds ( $SD = 32.17$ ). A paired  $t$ -test shows a significant difference in task completion time ( $t(47) = 10.07, p < 0.001$ ) with MultiNet achieving the lower mean times.

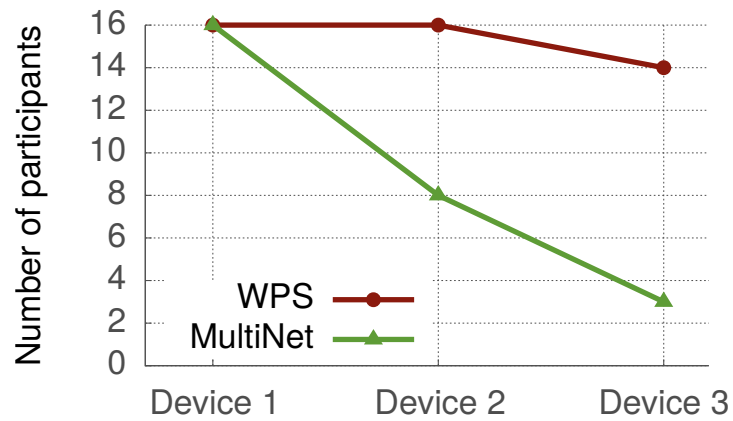
Observed instruction usage is shown in Figure 3.6b. Observing the trends shown in Figure 3.6, task completion times decrease in proportion at least as quickly with MultiNet as with WPS; and there is a marked decrease in instruction use with MultiNet, from 16 to 3, compared with the small decrease from 16 to

---

<sup>1</sup>One participant experienced a hardware failure while configuring the laptop with WPS so that data point has been removed.



(a) Average completion time (s) per device for both tasks.



(b) Participants' use of instructions.

Figure 3.6: Evidence for the learnability of MultiNet.

---

14 for WPS. This suggests that users found the consistent point and connect interface of MultiNet easy to remember and learn.

## 3.4 Network performance

The purpose of our performance measurements is to examine the feasibility of MultiNet for deployment in domestic environments given that the high number of virtual access points it creates is outside the expected operating envelope of the protocols and components.

### 3.4.1 Method

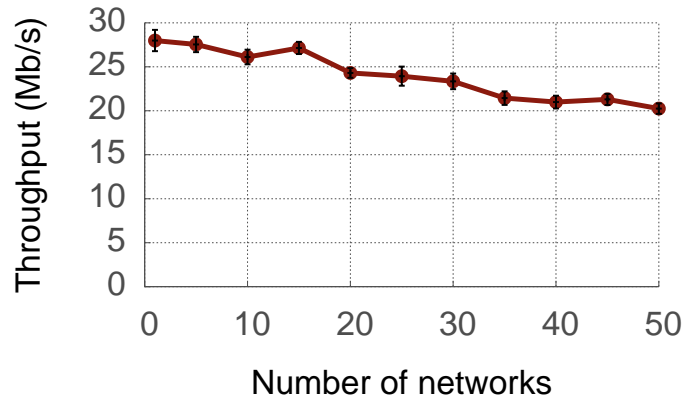
We constructed a test environment to measure throughput, latency and jitter as the number of connected devices (and thus configured virtual access points) increased. These metrics were chosen as they are standard indicators of network performance. We used 27 identical Samsung R5800 laptops with fresh installs of Microsoft Windows 7 as clients, and an eeePC netbook as the access point.

The standard networking tools *ping* and *iperf* were used to measure latency, throughput (over TCP) and jitter (over UDP). For each of these three performance indicators we configured the access point to offer the required number of networks and to act as a traffic sink. The first Samsung laptop is configured to act as a traffic source. Measurements were taken over a 60 second period after which the access point was re-configured and the experiment repeated, each time with an additional virtual access point created. We then repeated the whole experiment three times to generate the full dataset.

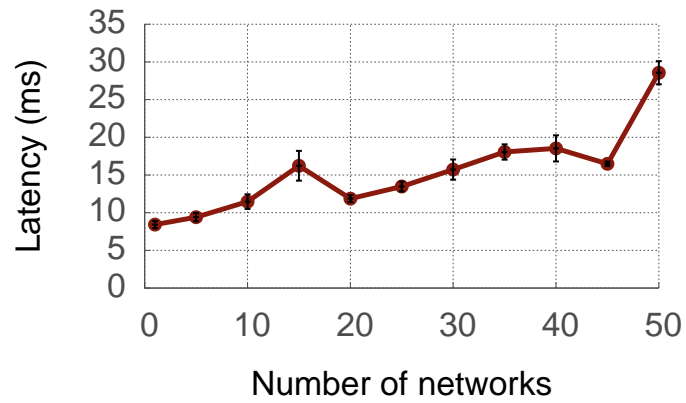
### 3.4.2 Results

Figure 3.7a shows the access point to device **throughput** displays approximately linear reduction as the number of networks and associated overheads increases, as expected. At 20 networks there is a 13% reduction in maximum throughput, and by 50 networks this figure has risen to 27%.

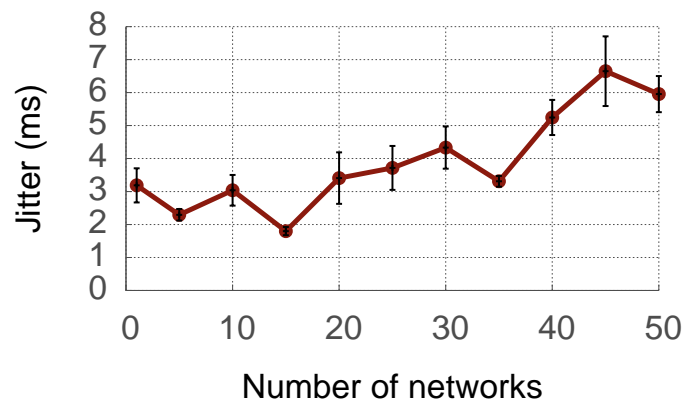
As the number of networks increases the **latency** on the networks also increases from 8 ms to 15 ms for up to 20 networks (Figure 3.7b). Although there



(a) Throughput



(b) Latency



(c) Jitter

Figure 3.7: Device to access point network performance as the number of configured networks increases. The mean  $\pm$  standard error is shown

---

appears to be the expected linear upward trend in per-packet latency as the number of networks and associated overheads increases, the degree of variation observed suggests that there are more significant factors directly affecting per-packet latency.

The **jitter** increases notably for more than 30–35 networks, but seems relatively constant when the number of networks is below that (Figure 3.7c).

These results quantify the performance of MultiNet, the increase in jitter and latency and drop in throughput will impact different types of protocols running over the network in different ways. To understand the impact of these findings on the network we examine their affect on four main activities seen on a typical network real-time streaming, web traffic and HTTP video streaming.

**Real-time streaming** protocols such as those used in Vice Over IP (VoIP), gaming and real-time video streaming, for example, Real Time Streaming Protocol (RTSP) [78], are sensitive to throughput, latency and jitter. VoIP and gaming have lower throughput requirements then video streaming. A minimum of 5 Mbit/s is recommended for High Definition content streaming <sup>1</sup>. MultiNet is capable of delivering these speeds even when 50 networks are enabled.

However, real-time protocols are also effected by latency and jitter. Some types of gaming are latency sensitive, for example, first person shooters. Larger latencies, over 100ms, can reduce the players' performance in these games [40]. At 50 networks Multinet adds 29ms to the overall latency. Depending on the location of the gaming server typical broadband latencies are between 30ms and 100ms [84]. Therefore, the addition of an extra 29ms delay could be problematic for this type of traffic in some cases. Jitter has less impact on gaming traffic with values in the range of 100ms having been shown to be acceptable [6].

Real time video streaming and VoIP protocols can be severely effected by jitter. Many of these protocols are dynamic altering the size of buffers and bitrates in response to changes in network conditions. High jitter can make it difficult for the adaption algorithms to settle on the correct type of action which can lead to a poor user experience [90].

**Web traffic** generated via normal web browsing has bandwidth requirements well below the levels that MultiNet provides. Modern web application page load

---

<sup>1</sup><https://help.netflix.com/en/node/306>



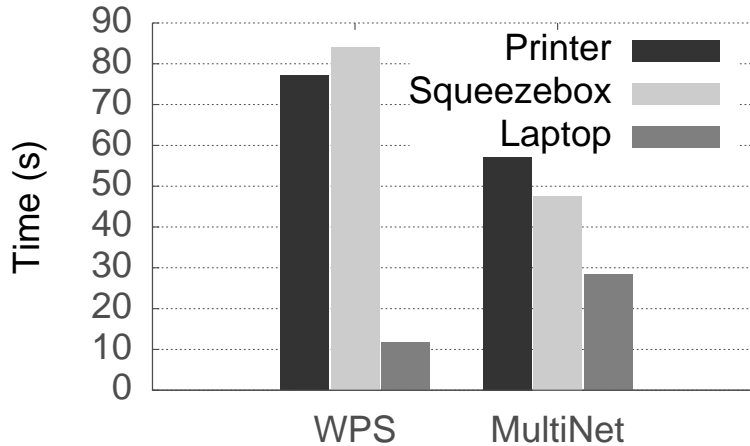


Figure 3.8: Average device connection time (s).

times are in the range of 5 to 20 seconds [92]. Hence the addition of a 29ms delay is unlikely to significantly impact performance.

**HTTP video streaming** has become the default delivery method for video content over the internet, with services like YouTube, Netflix and Iplayer using the Dynamic Adaptive Streaming over HTTP (DASH) protocol. These have been shown to be resilient to high latency and jitter [14, 53]

Overall these measurements show that MultiNet has a limited impact on network performance for less than 25 networks, supporting its feasibility for deployment into the home.

### 3.5 Device connection time

Device connection times for MultiNet and WPS were also measured, to check that MultiNet’s performance is comparable to existing systems. These measurements were performed on the test setup described in the user study. This was motivated by the need to check there were no adverse effects on device connection time with different device types.

Device connection time has two components: the time required for the user to complete the appropriate configuration steps to initiate device connection, and the time taken for the relevant key exchanges and network configurations to take

---

place to securely associate the device with the network. The first is measured in our user trial, presented in Section 3.3. The second is independent of the user, and is measured from the last step in the configuration process to the point at which the device receives an IP address from the DHCP server running on the access point.

This test was performed 16 times per device and averages calculated and shown in Figure 3.8. In the case of the printer and Squeezebox, the average device connection time is notably lower with MultiNet compared to WPS, but the Windows 7 laptop connects more quickly with WPS than with MultiNet. This is because the laptop connects when Windows 7 detects presence of the pre-configured wireless network as it polls for available wireless networks, in contrast to the user initiated action of connecting via WPS. If the user were to boot the laptop after configuring the network, or were to manually initiate a poll, we expect the connection time for the laptop would come down.

## 3.6 Discussion

This chapter sets out to answer Question 1.0: Are user-centred mechanisms for infrastructure control beneficial for domestic networks? To address this question one aspect of domestic infrastructure interaction was chosen to focus the work, specifically Wi-Fi device association. This chapter has presented and evaluated *MultiNet*, a new user-centred mechanism for joining devices to domestic wireless networks. This discussion will highlight the findings and discuss the outcomes for future domestic infrastructure deployments. To answer question 1.0 it was broken down into four sub questions. Each will be discussed in turn below.

The first question was Q2.1: How should Wi-Fi device association be changed to better fit domestic environments? It was evident from the literature that Wi-Fi device association in domestic environments was troublesome, especially for devices with limited interaction capabilities. In section 3.1 literature relating to domestic networks and Wi-Fi device association were reviewed and ten design parameters were drawn up to guide the redesign of the device association process. These design parameters covered three main areas. Firstly, the limitations of non-technical domestic users. Second, contextual issues related to the

---

domestic environment. Finally, technical issues such as the need for backwards compatibility. These ten design parameters were then used to redesign the device association process for domestic users. These design parameters highlight the important factors at play in domestic Wi-Fi device association and answer the question posed.

Once the design parameters were set, the process of redesigning and implementing Wi-Fi device association provides the answers the Question 2.2: What changes are required to the domestic network infrastructure to implement a user-centred Wi-Fi device association method?. The benefits of out-of-band credential exchange in this context were obvious from the literature, but how to implement one without placing extra hardware burden on the devices and without breaking backwards compatibility was the first challenge that had to be overcome. The concept of configuring the network to the device was key to overcoming this barrier. All Wi-Fi devices can store Wi-Fi network credentials. If a mechanism can be found to pass credentials from a device to the access point then a network could be created with the preconfigured credentials for the device to associate with. It was known that the access point software could offer more than one network per access point, but whether the upper limit existed was unknown. A review of the 802.11 specification [4] uncovered a suggestion of a maximum of four networks in a footnote. However, there was no concrete recommendation.

The code for the Atheros 802.11n Wi-Fi chip-set was reviewed and it could be seen that the four device limit was implemented in the driver, but it could be changed. Changing this for a higher number had no obvious impact on performance and allowed the creation of many networks. After making this change it was possible to create and manage many networks with *hostapd*. However, there was a small problem. MultiNet required the new network to be added without interrupting other devices on other networks offered by the same *hostapd* daemon. By design *hostapd* disassociated all stations on all networks if its configuration is changed. Hence, *hostapd* was modified to only disassociate devices on a network if the network configuration had changed. These changes enabled the creation of many networks. However, a method to create the out-of-band channel without introducing hardware constraints on devices was still required.

---

Creating an out-of-band channel for credential exchange without introducing hardware constraints on devices was achieved by introducing a third device into the association process, the *Network Controller*. The *Network Controller* can accommodate any hardware required to implement the out-of-band channel that we chose and provide, in this case a QR Code reader. The *Network Controller* also provides an interface to the network to display relevant information and provide a user interface. The implementation described here used a mobile phone as the *Network Controller* to offer a low-cost upgrade path.

However, the concept of configuring the network to the device could be implemented using other proximate out-of-band transfer techniques. For example, one could easily replace the QR Codes with credentials encoded on a USB storage device. In this scenario plugging a USB device into the access point would act as the out-of-band channel, allowing the correct network to be configured on the access point without need for a *Network Controller*. Adding the *Network Controller* also meant adding an method for the access point and *Network Controller* to communicate configuration changes. This was achieved using a *Network Controller* specific WPA2 secured network over which a RESTful API was exposed, providing the *Network Controller* access to the functionality of the access point.

These changes allow the implementation of a Wi-Fi device association method for domestic environments that meet all ten of the design parameters outlined in section 3.1. The changes to implement MultiNet were substantial. They involved modifications to hardware drivers, user space daemon responsible for access point and authentication functionality, the addition of new hardware and APIs. The access point was significantly modified and new functionality was added to fulfil the requirements of a user-centred mechanism for Wi-Fi device association.

However, all of the changes were in the software and none of the security critical parts of the WPA2 protocol needed to be modified. This shows that software changes to the underlying software supporting the domestic network infrastructure can enable radical changes in the user interaction.

The changes required to implement MultiNet were significant. Moving to a configuration with one network per device could potentially have a detrimental effect on overall network performance. To understand this and answer Q1.3:

---

What are the network performance implications of the redesigned infrastructure?, a performance evaluation of MultiNet was undertaken.

This evaluation suggests that MultiNet is technically feasible. Although there is a negative impact on throughput, latency and jitter, it is acceptably small for up to 25 devices. While a 25 device cap is a limitation of MultiNet, this should not significantly affect today's domestic wireless deployments: participants in our user trials reported a mean of 5.6 devices connected to their home networks, which tallies with the 4.3 devices found in the *2011 Connectivity Report* that surveyed a thousand UK homes [76].

The observed performance loss requires further analysis, but our hypothesis is that it may be related to both 802.11 beaconing interval and re-keying time. A review of the *hostapd* software reveals that the beaconing intervals are configurable but the final determination of how and when they are sent is left to the device driver. In the case of the ath9k driver used in these experiments there are two modes of operation depending on the hardware version “For multi-bss ap support beacons are either staggered evenly over N slots or burst together” (Line 491 drivers/net/wireless/ath/ath9k/beacon.c). It is unclear which strategy was in use in our hardware. Further investigation would be required to resolve this issue.

From the performance evaluation we can see that the modifications required to build MultiNet have had a negative impact on overall network performance. However, whether or not the usability improvements outweigh the performance decrease would require further investigation with users.

Question 1.4: How the usability of the new method compares to existing device association methods is a key question. Significant effort has been expended to design and build a user-centred mechanism for Wi-Fi device association. MultiNet has two key modifications which aim to improve its usability in domestic environments. Firstly, configuring the network infrastructure to the device and introducing a *Network Controller* has enabled a consistent configuration metaphor without imposing new hardware or software constraints on devices, and maintaining backwards compatibility with existing equipment. Second, MultiNet also addresses the diverse, and often limited, interaction capabilities of modern networked domestic devices by moving the configuration task from the devices

---

to the *Network Controller*, in effect creating a single point of configuration for joining any device to the network. This is achieved by creating and maintaining multiple virtual access points.

The user trial shows that both WPS and MultiNet performed well in a lab environment and all of the participants managed to complete the entire task in both conditions. However, MultiNet produced significantly better SUS scores across the trial, and all participants stated that they preferred MultiNet over WPS. The dramatically reduced instruction usage observed as participants moved through the task with MultiNet is an indication that the consistent interaction approach was readily learned by users.

The qualitative comments also suggest a preference for the use of a *Network Controller* and that this was more easily applicable to people's domestic deployments where access to the access point is often limited. The participants also highlighted a number of real world issues with WPS, commenting on the problems arising from the spatial arrangement of the networking infrastructure in their homes and its unsuitability for distributed devices. One limitation of the user study is that the usability of bootstrapping the *Network Controller* was not considered. It was felt that this was not necessary as the boot strapping is a one-off task that uses a roughly similar interaction to normal device association.

The overarching question this chapter set out to begin to address is Q1.0: Are user-centred mechanisms for infrastructure control beneficial for domestic networks? While this chapter does not fully answer this question, it has been shown that by redesigning network infrastructure to create user-centred mechanisms for infrastructure control, in the case of Wi-Fi device association, it produces a different association mechanism. That, in lab based usability tests, has been shown to improve usability over the currently deployed methods. This is an encouraging result that shows that if users have the correct infrastructure, network management problems can be resolved. The approach taken in this chapter has merit in this case. Applying user-centred design principles to other issues within domestic networks may also yield interesting results.

---

## 3.7 Limitations

One presumption in the design of MultiNet is the availability of a *Network Controller*. The *Network Controller* is required to complete the configuration process and reusing an existing device offers a low cost path to adoption. We envisage this actually being an app on a mobile device such as a smartphone, analogous to the approach taken by Cisco in their “Connect Cloud” platform.

However, the concept of configuring the network to the device could be implemented using other proximate Out-of-Band transfer techniques. For example, one could easily replace the QR Codes with credentials encoded on a USB storage device. In this scenario plugging the USB device into the AP would act as the Out-of-Band channel, allowing the correct network to be configured on the access point without need for a *Network Controller*.

The performance evaluation of MultiNet is not complete. More work is required to locate the root cause of the observed performance decrease. Further performance evaluation is also required to assess the impact of MultiNet on a busy network with many devices.

In the next chapter, user-centred presentations of network activity are explored. A new technical probe, HomeNetViewer, is constructed using a user-centred design approach. HomeNetViewer’s goal is to investigate user-centred presentations of network activity with the aim of improving domestic network legibility.

## Chapter 4

# User-centred presentations of network activity

This chapter explores the use of user-centred presentations of network activity to improve domestic network legibility. The empirical studies by Tolmie et al. show that domestic network use is controlled by the creation of locally negotiated policies between the members of the household [26]. These rules are often not expressed in the network: they live in the social fabric of the household.

Brundell et al. also found that users discuss and characterise their network usage not around protocols or forms of traffic, but rather, specific applications and activities performed on the network [18]. The enforcement of these rules are flexible and are often a negotiation between the occupants of the household.

In contrast, the tools currently provided to manage domestic networks are based around abstractions useful to trained network administrators. Their vocabulary is one full of technical terms such as port numbers, MAC addresses and IP addresses. The rules that can be expressed and enforced using these tools are inflexible.

The challenge this chapter addresses is not how to encode the rules and policies required by domestic users in the network infrastructure, but how to support users in the social task of understanding and monitoring their networks. This approach is in line with that suggested by Crabtree et al. [26]. This chapter sets



---

out to achieve this by continuing the theme of reinventing the domestic network infrastructure to support self-management by domestic users.

In this chapter the design, construction and evaluation of a system for user-centred presentation and annotation of network traffic is presented. Inspiration for this work came from the findings of Costanza’s work with domestic energy consumption data [22]. Costanza found that by using time-series historical visualisation for energy data with user annotation that users’ could better relate complex energy data to their everyday lives. This finding provides an interesting starting point for the development of a domestic network data visualisation platform. Costanza’s work relates energy data to physical actions. This chapter explores how to relate network data to online actions, with the aim of improving users’ understanding of their network usage.

The approach taken is to provide an interface to visualise what has happened or is happening on the network and allow users to annotate features they find interesting in the traffic. The annotation of interesting features will provide a record of events on the network, annotated in the users’ own language. It is envisaged that this will enable users to easily inspect what has happened on their network to ensure local rules are being adhered to. This chapter addresses the following questions:

**Q3.0** Do user-centred presentations of network data improve network legibility?

**Q3.1** Of the data flowing through the domestic network access point, which are best suited for use in user annotation?

**Q3.2** Are interactive time-series historical visualisations appropriate in the context of domestic network data?

**Q3.3** Is the use of activities, applications and users an appropriate language to annotate domestic network data?

**Q3.4** How do users feel about the increased network legibility?

To address the above questions this work is split into four phases. Firstly, the initial design phase, where user-centred design practices and local expert knowledge are applied to develop a system to visualise and annotate home network data

---

called HomeNetViewer. Data collected in a previous Homework deployment [63], in real UK households, is used to create the first prototype of HomeNetViewer. This enables questions Q3.1 and Q3.2 to be explored.

Second, the iterative design phase, where the prototype system is incrementally improved with a single domestic user from the household who provided the initial data. The third phase is a set of controlled deployments to road test HomeNetViewer before the final phase. Finally, the deployment phase, where HomeNetViewer is deployed in four real UK households to begin to address Q3.3 and Q3.4. In the next section the initial system design is presented.

## 4.1 System design

In the design phase a user-centred approach is taken to the construction of the visualisation and annotation interface. The initial interface was developed using five months of traffic captured at a single family household in 2012 using the Homework router platform [63]. Firstly, this section outlines the factors at play for a domestic network data visualisation and annotation platform, in terms of the audience, purpose, context and systems. This will provide an overview of the context in which HomeNetViewer is deployed and will inform the initial system design.

**Audience:** the audience for HomeNetViewer are domestic network users, specifically ones that need to negotiate acceptable use of the domestic network. The literature shows that users of domestic networks are often non-technical and have no desire to become networking experts. The typical user is familiar with the Internet, but not the underlying technical infrastructure. The audience for this system is envisaged to be mainly parents, but not exclusively. Other types of households may also find increased visibility beneficial. For example, a shared household may wish to use this system to resolve bandwidth contention issues.

**Purpose:** the purpose of the system is to support domestic users in the generation and monitoring of locally negotiated network rules and policies. The system should provide users of domestic network with a simple method to navigate and annotate their network data. The system will use interactive time-series historical visualisation as the main interface and activities and users as the annotation

---

meta-data. These annotations can then be used as a view of what is happening and what has happened on the network. The main goal of the visualisation is to enable the users to check that locally negotiated policies are being followed.

**Context:** the domestic context is a complex socio technical system. Each household is different in terms of the technology deployed, the number, types, and manufacturers of devices. There will be a mix of wired and wireless devices and these may be mobile or used at a fixed location within the home. The way in which the devices are used also varies between households depending on the goals of its users. In domestic households devices are also often shared, used by many users, sometimes in groups or by individuals.

**Systems and data:** currently deployed domestic access points are often limited in computational power and storage capacity, although recent trends toward App-enabled routers are moving in the direction of increased computing power and functionality. The home access point is an important piece of the domestic infrastructure. Hence, reliability and performance are important considerations.

This work aims to create user-centred visualisations of the data flowing through the domestic access point. Therefore, the access point needs to be modified to collect and store the data passing through it. Rather than constructing this from scratch this work builds upon the Homework router platform [63]. The Homework router platform is used to provide Wi-Fi, routing and data logging functionality.

Homework is built on an Eee-PC running Ubuntu. Homework utilises Open vSwitch<sup>1</sup> for forwarding and OpenFlow<sup>2</sup> to manage the behaviour of the switch. It provides logging of Wi-Fi RSSI, HTTP traffic(via DPI), IP Flows, DHCP Leases, and connected devices. Details of the data collected and how the collection was implemented are provided below:

*Wi-Fi RSSI* is the Received Signal Strength Indicator. An integer value between 0 and 100, representing the power of the receive signal at the end station or client device. The RSSI is calculated by the 802.11 compliant hardware on the client device and reported back to the home access point. There is no defined standard for the generation of the RSSI value. Therefore, different devices may report different values when receiving the same signal at the same location.

---

<sup>1</sup><http://www.openvswitch.org>

<sup>2</sup><https://www.opennetworking.org/sdn-resources/onf-specifications/openflow>

---

However, high RSSI values are associated with a strong signal and good network performance and low values are a indicator of poor performance. The relationship between performance and RSSI make this an important property for troubleshooting Wi-Fi performance problems. The RSSI information is part of the 802.11 physical layer, so to extract it we require access to the raw 802.11 frames. Frame interception is achieved using Radiotap<sup>1</sup>, a tool that allows the injection and reception of raw 802.11 frames on Linux. For each frame received the RSSI is extracted and stored along with the client MAC address and frame timestamp into the Homework database. This functionality was provided as standard by the Homework platform.

*DHCP Leases and connected devices:* DHCP Leases are generated when a device joins the network and uses the Dynamic Host Configuration Protocol to receive configuration information. DHCP is responsible for the allocation of IP addresses on the local network. The DHCP service was provided by the Dnsmasq daemon<sup>2</sup> and logging was provided by the Homework platform. For each DHCP event Homework logged event timestamps, client MAC address, client IP address, client hostname and event type. The event type was either add or delete. The event records can then be processed to provide time ranges describing when each device held a particular IP address.

*IP Flows:* a Flow is defined as “a set of IP packets passing an Observation Point in the network during a certain time interval. All packets belonging to a particular Flow have a set of common properties.” [21]. In this case the Observation Point was the domestic access point. Each request to and response from a remote server would generate an IP Flow record which was timestamped and stored in a database on the access point for later retrieval.

*DNS requests:* Domain Name System requests are generated whenever a client on the network needs to convert a host name into an IP address. The DNS service was provided by the *Dnsmasq* daemon and logging was enabled. The DNS logs were periodically parsed and hostname to IP address mappings were extracted. These mappings are very valuable, especially in the case of web browsing, as the hostname looked up in the DNS request is the one entered by the user.

---

<sup>1</sup><http://www.radiotap.org/>

<sup>2</sup><http://www.thekelleys.org.uk/dnsmasq/>

---

This is important as it can be used in place of a reverse DNS lookup which converts an IP address back into a hostname. Reverse DNS lookups have two limitations which make their use undesirable. Firstly, they are slow to perform. Second, the hostname they return are not necessarily the same as the host name looked up, due to the use of DNS based load balancing in modern network applications. One other limitation of DNS logs is that many client devices cache DNS requests. Hence, the DNS logs do not provide a full picture of the number of times a particular host is contacted.

*HTTP traffic:* the Homework platform collects HTTP traffic information using deep packet inspection techniques. It extracts the HTTP headers from the packets captured using *libpcap* as they pass through the access point. For each HTTP request the system logs the current timestamp, protocol, source IP address, source port, destination IP address, destination port, server hostname and the full URL including the query string. For hosts accessed using HTTPS it is not possible to access the hostname, URL or query string, so these are not present in the logs.

The above section provides an overview of the context into which the system will be deployed. The next section discusses the ethical implications of deploying this system into peoples homes.

#### **4.1.1 Ethical considerations**

Early on in the design phase of the work a number of ethical issues were raised. These affect the design choices and evaluation of HomeNetViewer. The main ethical concern is that HomeNetViewer changes the visibility of domestic network activity. The currently deployed systems offer little or no insight into the data flowing through the network. Hence, most activities are hidden from other users in the household.

HomeNetViewer changes this and will make all activity visible to some degree to all users of the domestic network. This increased visibility leads to the possibility of causing embarrassment to the participants. Embarrassment may arise for two reasons. Firstly, if data seen by an another family member exposes an activity considered unacceptable within that household. Second, if a matter

---

considered private by a user is exposed to another user. For example, a medical condition.

A number of approaches were explored to address the potential for embarrassment. Firstly, a pro-active approach was considered, where users could opt-out of data logging for a particular device before performing certain activities. This requires planning and foresight on part of the user and could easily be forgotten. Therefore, it does not fully mitigate the risk of embarrassment.

Another approach considered was to hide all data until a user agrees to make it public within the household. However, this approach is fundamentally flawed. The system does not know which user generated the traffic. Therefore, it cannot know who to ask for permission to release the data.

The final approach examined is a retrospective solution allowing users to remove traffic they do not wish others in the household to see. While this has some benefits over the other methods it still leaves a window of opportunity of embarrassment to be caused.

None of the explored approaches were perfect and a combined approach would have probably been the best solution. However, this would have significantly increased the complexity of the interface and potentially affect data quality. Hence, a pragmatic approach was adopted.

During the deployment of HomeNetViewer it was ensured that all participants were fully aware of the data that could be seen within the system and informed that anyone in the household could see these data. All members of the household were asked to sign a consent form agreeing to this and extra care was taken when explaining the system to children and young adults. Participants were also able to withdraw their consent any time. If just one member of any household withdrew the whole system would be removed from the household and the data destroyed. This approach was deemed acceptable by the Ethical Review Committee responsible for the School of Computer Science at The University of Nottingham.

In the next section the development of the initial HomeNetViewer prototype is presented.

---

### 4.1.2 Prototype interface

The starting point for the prototype of the HomeNetViewer platform is the interactive time-series historical visualisation used by Costanza for domestic energy consumption data [22]. However, the data flowing through the domestic network are significantly different and more complex than the data available from domestic energy monitors. Domestic network data have many values at a single point in time representing different activities taking place on a device, in contrast to the single energy consumption figure visualised in Costanza’s work.

The first step was to look for data that could be easily represented on a simple time-line. Wi-Fi RSSI and incoming and outgoing bandwidth were the obvious choices. A simple interface displaying these on a time-line was constructed. The ability to “drill down” into the lower level activity at a particular point in time was then added. This took the form of a pop-up window displaying the raw data from the DHCP, DNS, IP Flow and HTTP traffic logs.

The early attempts at visualising this data quickly became cluttered and overloaded with technical information, such as port numbers, IP addresses, and MAC addresses. It was clear that we needed to reduce the complexity of the data to build a usable visualisation. Traffic on port 80 accounted for approximately 53% of all IP Flows with another 6% on port 443. These correspond to HTTP and HTTPS respectively. The remaining 41% of IP Flows were distributed over 57,248 other ports. For example, port 53 (DNS) accounted for 0.7% of IP Flows. Given the dominance of HTTP and HTTPS traffic in the dataset it was decided to focus the interface on exploring this, rather than traffic on all ports. One benefit of focusing on HTTP is that users are somewhat familiar with its main identifying features: the URL, and the host and domain names they contain. HTTPS traffic was not included in this prototype as the logging mechanism relied on deep packet inspection and therefore was unable to extract data from the packets due to the encryption.

The focus on HTTP traffic does not mean the rest of the traffic is completely hidden. Non-HTTP activity, for example Skype and Bit-torrent, leave traces in the HTTP logs. These clues take the form of either visits to related websites (e.g. BitTorrent search engines) or accessing interface and updates over HTTP (e.g.

---

Skype’s interface is an embedded web page). It was also possible to see periods of high bandwidth which is an indication of activity on the network.

After the basic visualisation interface had been built the functionality to collect annotations from users was added. The prototype interface allowed collection of, device ownership, user ground truth and activity ground truth annotations as free text. The annotation interface consisted of a set of time-lines for each device connected to the network.

Each set of time-lines were labelled with the device hostname, where available, or the device MAC address if no hostname was captured. The devices could be renamed by the users to a more human friendly name if required. It was also possible to assign an owner to each of the devices in the interface. The time-lines represented Wi-Fi RSSI, bandwidth (inbound and outbound) and annotated HTTP visits along with other annotations added by the users. An interface was constructed to allow any section of the time-line to be selected and inspected in more detail using a wizard style interface.

In the detailed view users were shown a nested list of all the remote hosts that were contacted in that time frame grouped by domain name. Users were instructed to examine the list to find a domain/host that they recognised. They were then asked to add “tags”, relating to the activity most likely to have caused them to visit that domain/host. Tags were entered as free text with a list of previously entered tags displayed to improve consistency and reduce duplication. After this process users were taken to another screen where they could see the annotations they had just created on a time-line, and add extra information on which users were using the device and what they believed they were doing.

The prototype interface was shown to a number of local networking and HCI experts and two important changes were made. Firstly, it was noted that the domain/host annotation interface was cluttered with a large number of HTTP requests related to the delivery of online advertising. These made it more difficult to scan the list and find the domains/hosts of interest to human activity. Using a freely available list of advertising domains created to enable adverts to be blocked<sup>1</sup> we were able to filter out some of the advertisement related traffic. This reduced the number of domains/hosts displayed to the user by 17%.

---

<sup>1</sup><http://pgl.yoyo.org/adserver/>



---

Second, it was also noted that the URLs extracted from the HTTP headers contained more information than just the domain/host. For example, the full path of the page and data submitted using the GET method were also available. This includes search terms entered by users into search engines like Bing and Google. It was hypothesised that search terms would provide valuable contextual information for human annotation so it was decided to add this information into the interface. Search terms were extracted from major search engines (Google, Bing, Yahoo) and shopping sites (Amazon, E-bay). These were then displayed on the interface as blue dots on the device time-line. When the user moved the mouse over the blue dot the extracted search term was displayed.

At this stage a working prototype system for collecting and visualising domestic network data had been created. It was possible to include a prospective user into the design process. This was achieved through three iterative design sessions were undertaken with the data owner. This iterative design process, and the modifications made as a result, are described in the next section.

### 4.1.3 Iterative design with home-owner

After improving HomeNetViewer based on local expert feedback, one occupant from the household where the original dataset was collected was recruited to take part in a study. The study aimed to explore their network data using the prototype HomeNetViewer interface. This study took the form of three one-hour iterative design sessions. The first focused on the user interface, the second focused on the annotation process and the final session was to perform a full annotation of three weeks of traces.

The participant was compensated with a £25 Amazon voucher for any inconvenience. These sessions led to a number of usability improvements to the interface and an opportunity to observe a real user annotating their own data. Next we discuss the observations from each session, the impact on the system and where appropriate how the system was changed in response.

**The first session** focused on the interactive visualisation and data navigation. The participant was comfortable with the time-line view and generally understood what was being displayed without any prompting. The ability to

---

move backwards and forwards through the data one day at a time was considered useful.

However, the participant was frustrated that they could not see more of the data at once. They suggested that the addition of a week view and the ability to zoom out would be an advantage. Another issue raised by the participant was that they needed to do a lot of scrolling to view all of the devices.

Our initial interface showed all the devices on one page, with each device separated by a heading and horizontal rule. The household being examined had a large number of devices which led to very long pages. To address this issue, the interface was changed to a tabbed style with one device on each tab.

**The second session** focused on the annotation interface and leads to four interesting observations. Firstly, was specifically related to the annotation interface. The initial prototype was based on a wizard style interaction where the users was led through a series of screens and asked to input the relevant information. This quickly became tiresome as most of the screens were unnecessary if you only wanted to annotate a single piece of data. This caused a redesign of the interaction and interface around a toolbar containing four tools rather than a wizard of four screens.

The second observation was that device ownership is not an indication of exclusivity of use. When asked to assign an owner to any device that was for the sole use of one occupant, the participant stated that this was not possible. In this household some people are considered to own certain devices. However, it would not be unusual to find any member of the household using any device. The participant elaborated by saying “That’s my phone, and it’s mainly me who uses it, but quite often my wife will pick it up and do a quick google”. This fluidity of use is present across all devices in the participant’s household, therefore attributing traffic to a user solely based on the device is not possible in this case. Whether this is a trend across all households and device types requires the collection of more data. This observation did not directly affect the design of the system, but may have implications for the data analysis and provided a topic of discussion in the exit interviews.

The third observation was that some domains have a strong link to an individual user. On a number of occasions the participant stated that the site could only

---

have been visited by one member of their family. This observation led to the addition of the “host/domain user” tag to collect this information. These sites seem to appear multiple times in the dataset and are often related to specific interests. For example, visits to [soundsandgear.com](http://soundsandgear.com) and [deviantart.net](http://deviantart.net), were related to one householders music interests and another’s art hobby.

The fourth observation relates to the visualisation and access to search terms. These proved both interesting and controversial for a number of reasons. Firstly, search terms appear to be a good indicator of user activity. It was trivial for the participant to suggest the activity that generated each group of search terms shown on the interface. Second, search terms could in some cases be linked back to users, based on the content of the search and knowledge of the users’ interests. Third, search terms were good prompts for particular events, even though the traces were over one year old. On a number of occasions the participant was able to remember specific events and activities related to some of the search terms.

Finally, search terms were surprisingly intrusive. The participant expressed some discomfort at the level of information that was available. This discomfort was heightened as they seemed unaware that this information was present in the network traces. However, search terms also offer a real insight into the activities and interests of the users on the network there is one major limitation. The search terms are not machine readable, they are human input and often contain obscure references to places and people. Parsing and categorising them so that they would be usable in an automated fashion is an open question for the natural language processing community.

**The final session** focused on the annotation of a three week section of traffic data. The modifications suggested in the first two sessions were implemented in this version of the interface before the session. Overall feedback on the interface from this session was positive. The new streamlined annotation interface was much quicker to use, and the participant stated they found it a much less frustrating experience. Next, the test deployment of HomeNetViewer is discussed.

---

#### 4.1.4 Test deployment

After HomeNetViewer had been designed and built it went through a period of real world testing. The test deployments were in the researchers' homes to simulate the full deployment. This revealed one important problem. Since the collection of the data used to build the prototype, many search engines, shopping sites and social networks had moved to a default HTTPS policy. The Homework HTTP logger uses deep packet inspection to extract the URLs visited, but encryption prevents this from working. Hence, extracting domain names and search terms to display back to the users presented a significant technical challenge for the system deployment.

Three solutions to this problem were considered. The First solution explored was to perform a reverse DNS lookup on the IP addresses in the Flows table. This would convert the IP address into a human readable hostname for use in the interface. However, this was ineffective, due to the use of load balancing and content delivery networks. Due to the techniques used the reply from a reverse DNS lookup often bears no resemblance to the hostname entered in the URL by the user.

Second, the DNS lookups could be captured using a DNS proxy. The cached DNS lookup would contain the hostname entered by the users. This could then be used to annotate the IP Flow data retrospectively. This has the advantage of being unobtrusive, but it only allows us to perform host name annotations. Any analysis that requires deep packet inspection is still not possible.

The third solution is to use a transparent proxy that can perform a man-in-the-middle function, decrypting and encrypting the traffic as it passes through the domestic access point. This allows an opportunity to perform deep packet inspection and extract the information on the URLs visited and search terms submitted. This solution has the disadvantage that it breaks the expectation of the users that HTTPS is securely encrypted end to end.

Squid<sup>1</sup>, a widely used HTTP proxy, has the ability to transparently intercept HTTPS traffic using a module called SSL bump. Squid acts as a man-in-the-middle and intercepts any HTTPS CONNECT requests it observes. Squid then

---

<sup>1</sup><http://www.squid-cache.org/>

---

initiates one HTTPS connection from itself to the remote server using the standard SSL protocol and receives the requested data. The remote server certificate is then used with its own certificate to create a self-signed certificate which is used to encrypt the connection to the requesting client on the local network.

This self-signed certificate is not signed by a trusted Root Authority causing most web browsers and devices to display a certificate error. This can be overcome on desktop and mobile devices designed to be used in enterprise environments by installing the public key of the Squid certificate into the device key store and web browsers trusted certificate store.

This strategy works well in an enterprise environment. However, during the test deployment of HomeNetViewer some problems were encountered. Some closed consumer devices cannot be configured to accept new root certificates. In these cases some devices will just ignore the error and work as normal, but others do not and fail to operate as expected. Examples seen during testing were the Sky NOWTV box and the Sony PlayStation 4.

To overcome this we attempted to black-list the problematic domains identified above by excluding them from the HTTPS interception. Unfortunately, this was not possible. When deciding whether or not to intercept traffic the only information available to Squid is the destination IP address. IP address based black-listing is ineffective due to the use of load-balancing and content delivery networks that causes the IP addresses to change unpredictably over time. Host name based black-listing, is also not possible due the reverse DNS queries returning different host names to those accessed by the client.

The final approach adopted was to use a white-list. The DNS logs were used to extract the IP addresses for “sites of interest”. Sites of interest were chosen before the deployment and were sites that were expected to contain search terms (Google, Bing, YouTube for example). The IP addresses of the sites of interest were provided to Squid to enable HTTPS interception only for those addresses. This approach was successful, but had one draw back. The first time an IP was returned for a particular hostname of interest it would not be intercepted until the DNS logs had been parsed and the Squid configuration updated. This means that the first few requests over HTTPS for a site of interest are not available for deep packet inspection. For all other HTTPS traffic the DNS logs were used to

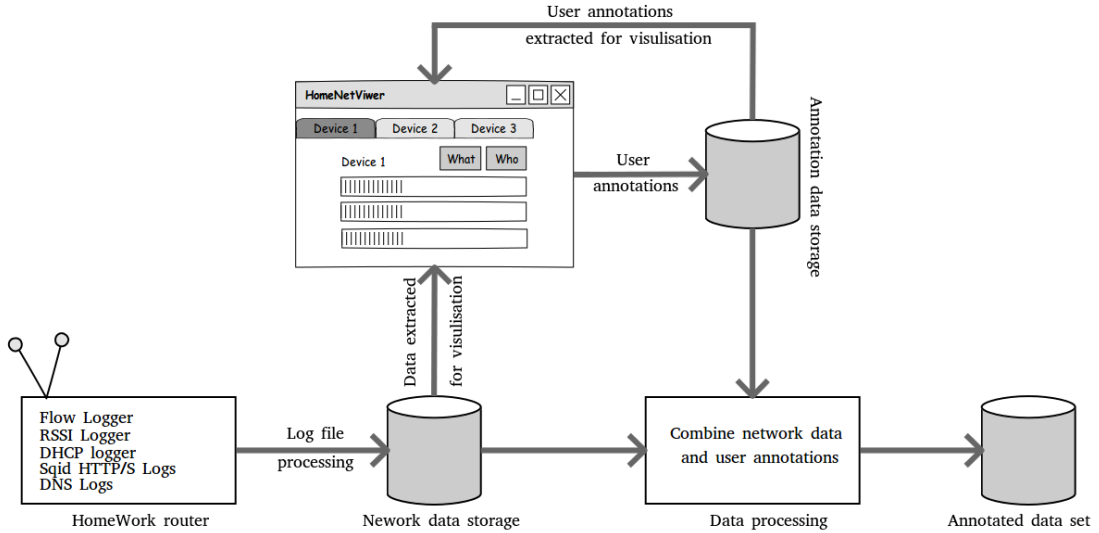


Figure 4.1: A system overview of HomeNetViewer data collection and annotation platform.

convert IP addresses into host names to provide as much information to the user as possible within the visualisation.

## 4.2 The final system

In this section a complete description of HomeNetViewer is presented as it was deployed into the participants' homes. An overview of the system can be seen in Figure 4.1. Firstly, a description of the interactive visualisation designed to enable the exploration of this data is presented. Finally, the annotation data collection interface is discussed alongside a description of the type of annotations collected and the data they contain.

### 4.2.1 Interactive visualisation

The interactive visualisation allows the manipulation of two dimensions, the device and time window. The default view is to display a set of stacked time-lines representing a one day period (an example is provided in Figure 4.2). Each time-line represents one data source generated from the raw data or user annotations.

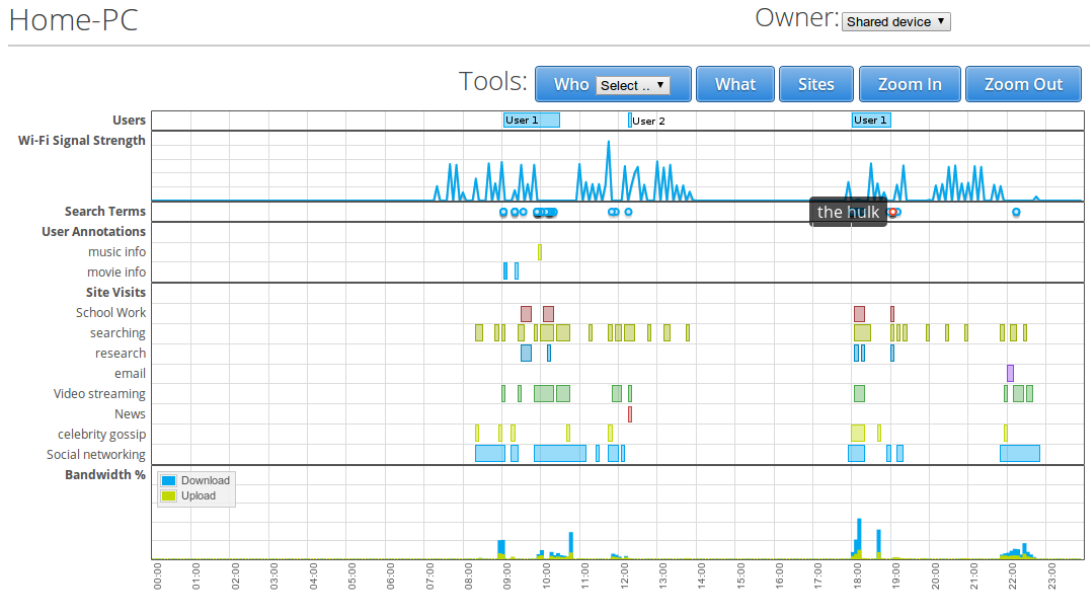


Figure 4.2: Final annotation interface for a single device.

The active device can be changed by selecting a new tab which is named with the device hostname.

The time window can be altered in a number of ways. Firstly, it is possible to switch between a one day and week view using a button on the top toolbar. Second, the user can step through the data using the next and previous buttons. The user can also select any section in the visible time window and zoom in to see a larger view presented in a pop-up window. Finally, the user can zoom out which doubles the time range shown each time the tool is activated. The visualisation also provides an aggregated view across all devices. This view shows cumulative representation of all the data collected from all devices on the network.

#### 4.2.2 Annotation capabilities

The interface was also designed to collect annotations, including device ownership, device usage, user annotations and activity ground truth annotations. There were a number of styles of activity and user annotations these are described below:

- **Host/Domain activity** annotations represent the activity the users attribute to the most likely cause for them to visit a particular domain/host.

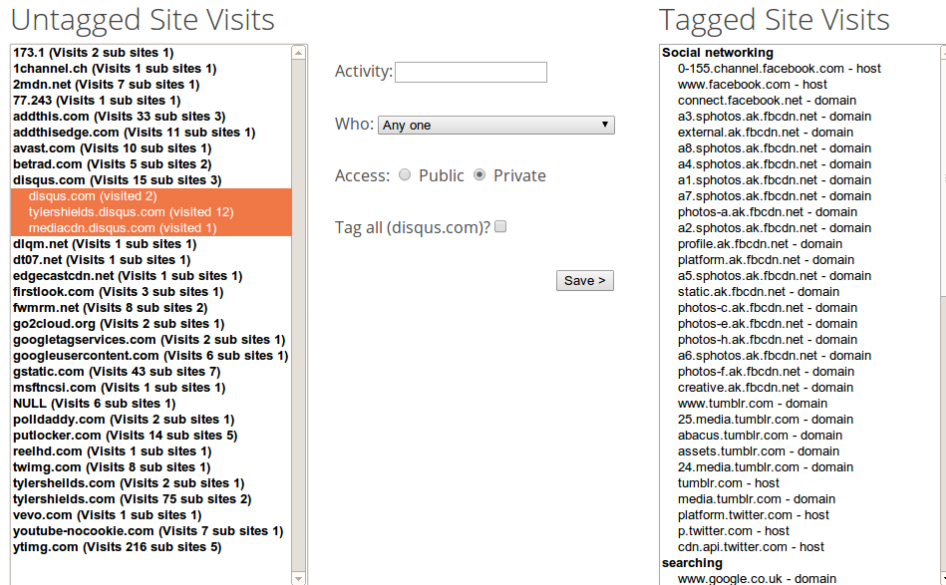


Figure 4.3: Host/domain annotation interface

- **Host/Domain user** annotations were designed to take advantage of the observation that some hosts/domains have a strong link to an individual. These tags represent the links between users and host and/or domains.
- **Search activity** annotations capture the knowledge of the annotating user concerning the most likely activity that could have generated a single search term.
- **Search user** annotations are based on the observation that some searches are easily identifiable as being generated by a specific user. These tags encode the link between a particular search and a user.
- **Free user** annotations were designed to allow self reporting of device usage by users.
- **Free activity** annotations allow users to self report the activity they were engaged in over a particular time range.

The main interface provides four tools to collect the above annotations: the what tool, the who tool, the sites tool and the searches tool. The tools can be



---

seen in the top left of Figure 4.2. These tools are all activated using the same user interaction. Firstly, the users select an interesting portion of the time-line using the mouse, then activates the desired tool by clicking on it in the toolbar. This highlighted section of the time-line could then be annotated. This select and activate interaction was chosen as it enables the vast amounts of data to be effectively filtered by time, reducing the complexity of the annotation task. Each tool is described in turn below.

**The what tool** is designed to collect per device free activity annotations. When activated a menu is displayed below the button. It contains a text-box to enter the activity and a set of radio buttons to toggle between public and private. When the user selects the text box a list of all previously entered activities is shown to enable the selection of repeated activities. The list of available options is filtered as the user types. When the annotation is saved the selected time range, enter tag, annotating user, device and visibility are saved to the database and the interface is updated to show the new annotation.

**The who tool** is designed to collect per device free user annotations. Once the user has selected the desired time range they can select the users from a drop down list. On selection the selected time range, selected user, annotating user, device are saved to the database and the interface updated to show the new data.

**The sites tool** is designed to collect host/domain activity tags and host/domain user tags. The interface can be seen in Figure 4.3. The nested list on the left hand side shows all the remote hosts that were contacted in the selected time-frame grouped by domain name that have not been tagged. Users can examine the list to find domain/hostnames that they recognise. They can then add “tags”, relating to the activity that most likely caused a visit to that site. This interface also allows users to be assigned to domains/hosts by selecting them from a drop down.

**The searches tool** is used to collect search user and search activity tags. When it is activated the searches logged in the selected time frame are displayed as an ordered list with duplicates removed. The user can then assign activity and user to any of the listed searches.

All the tools also provide a drop down list of previously entered tags, where possible. This was included to increase the accuracy and consistency of the

---

meta-data and reduce duplicate and mistyped entries. The tools also supported public and private annotations enabling the entry of private annotations which are hidden from other users. The next section describes the “In the wild” deployment of HomeNetViewer including how the system was deployed, the experimental method and a description of the participating households.

## 4.3 HomeNetViewer deployment

The real world deployment of HomeNetViewer has three main objectives. The first is to collect real world annotated domestic network data to explore the utility of interactive time-line visualisation for domestic users. The second objective is to explore users’ reactions to the visualisation platform and the increased transparency it affords. The final objective is to gather data on the language and terminology domestic users use to describe their network activity. Next an outline of the practicalities of the deployment are given.

### 4.3.1 Method

HomeNetViewer was deployed in four participating households for a period of three weeks. Three weeks was chosen to provide sufficient data for analysis while minimising the disruption for participants. Due to the length of the deployment and the intrusive nature of the data collection recruitment of participants proved difficult. This led to an opportunistic sampling strategy where interested households were recruited. However, attempts were made to recruit households of different demographics to improve the quality of the sample. Participating households were compensated with a £50 Amazon voucher for any inconvenience caused. The deployment consisted of three visits to each household. Next we detail the content of the visits.

The goal of the first visit was to perform the installation of HomeNetViewer and provide initial training to users. Installation consisted of several steps. Initially the existing state of the network was documented, to enable its reinstatement after the deployment. The existing Wi-Fi network was then disabled and HomeNetViewer configured with the same BSSID and passphrase to replace it.

---

This enabled all existing configured Wi-Fi devices to connect directly to HomeNetViewer. Wired devices were unplugged from the existing router and plugged into HomeNetViewer to enable their traffic to be captured. HomeNetViewer's uplink was then connected to the existing router via Ethernet to enable traffic to be routed through the existing Internet connection to the rest of the world.

The next phase of the installation was to install HomeNetViewer's public SSL certificate into all compatible devices key-stores and web browsers trusted root certificate stores. This involved manually configuring each device, at this point the connectivity of each devices was checked. The final stage of the installation was to check that all the other devices on the network such as streaming media boxes and networked printers were functioning as expected.

After installation all the family members were gathered and the basic operation of the interface was explained. The operation of each of the four tools was explained and the visualisation was explored. During training care was taken not to lead the participants into using any particular terminology to describe the data. During the demonstration, at points that required the entry of tags or annotations the participants were asked to suggest the terms used.

The second visit to the household was two days after the first visit. This was a quick follow up visit lasting approximately thirty minutes. Its main purpose was to ensure that the installation was performing as expected, the users were annotating their data, and to answer any questions raised by the participants' recent use of the HomeNetViewer.

The final visit took place three weeks after installation. The first task was to quickly review the annotated data with the participants to ensure that we had good coverage of annotations. The network was then returned to its initial state and HomeNetViewer was removed. After the deployment a set of semi-structured exit interviews were conducted with each household. The next section describes the participants recruited and the make-up of their domestic network infrastructure.

---

### 4.3.2 Participating households

HomeNetViewer was deployed in four real households in the UK for a period of three weeks. This section provides information on the social and technical make-up of the participating households. Participants' names have been anonymised to protect their identities.

**Household 1 (H1):** a four person family home with two adults and two school aged children, more information can be seen in Table 4.1. They had ten network connected devices that were in use during the study.

**Household 2 (H2):** a four person family home with two working adults and one school aged child, more information can be seen in Table 4.2. This household also had a second young adult who was away at university for most of the deployment period and returned for the weekend towards the end of the study. They had fourteen network connected devices.

**Household 3 (H3)** : a four person family home with two working adults and two school age children, see Table 4.3. They had twelve devices connected to their network.

**Household 4 (H4)** : a two person family home with two retired adults. They had 6 devices actively in use on their network.

User	Gender	Role	occupation	Age
H1U1	Male	Head of Household	Teacher	40-44
H1U2	Female	Child	Secondary School	15-19
H1U3	Female	Child	Further Education	15-19
H1U4	Female	Head of Household	Nurse	45-49

Table 4.1: Household 1 participant information

---

User	Gender	Role	occupation	Age
H2U1	Male	Head of Household	Phd Student	35-39
H2U2	Female	Adult	University Student	15-19
H2U3	Female	Child	Secondary School	15-19
H2U4	Female	Head of Household	Self Employed	40-44

Table 4.2: Household 2 participant information

User	Gender	Role	occupation	Age
H3U1	Female	Head of Household	Child Minder	35-39
H3U2	Male	Head of Household	Self Employed	40-45
H3U3	Male	Child	Secondary school	10-14
H3U4	Female	Child	Primary school	5-9

Table 4.3: Household 3 participant information

User	Gender	Role	occupation	Age
H4U1	Male	Head of Household	Retired Solicitor	65-70
H4U2	Female	Head of Household	Retired Academic	65-70

Table 4.4: Household 4 participant information

### 4.3.3 Results: data annotations

In this section the results for the deployment are discussed. Firstly, an overview of the annotations added to the data by the participants is presented before moving on to the results of the exit interviews.

	H1	H2	H3	H4
Host/Domain activity tags	98	135	47	42
Host/Domain user tags	29	32	47	34
Search activity tags	195	218	0	0
Search user tags	155	228	0	0
Free user	112	241	110	57
Free activity	0	124	103	43

Table 4.5: Annotations entered per household per annotation type

Table 4.5 shows the number of each type of annotation created by each household. We can see that most households used most of the annotation types. How-

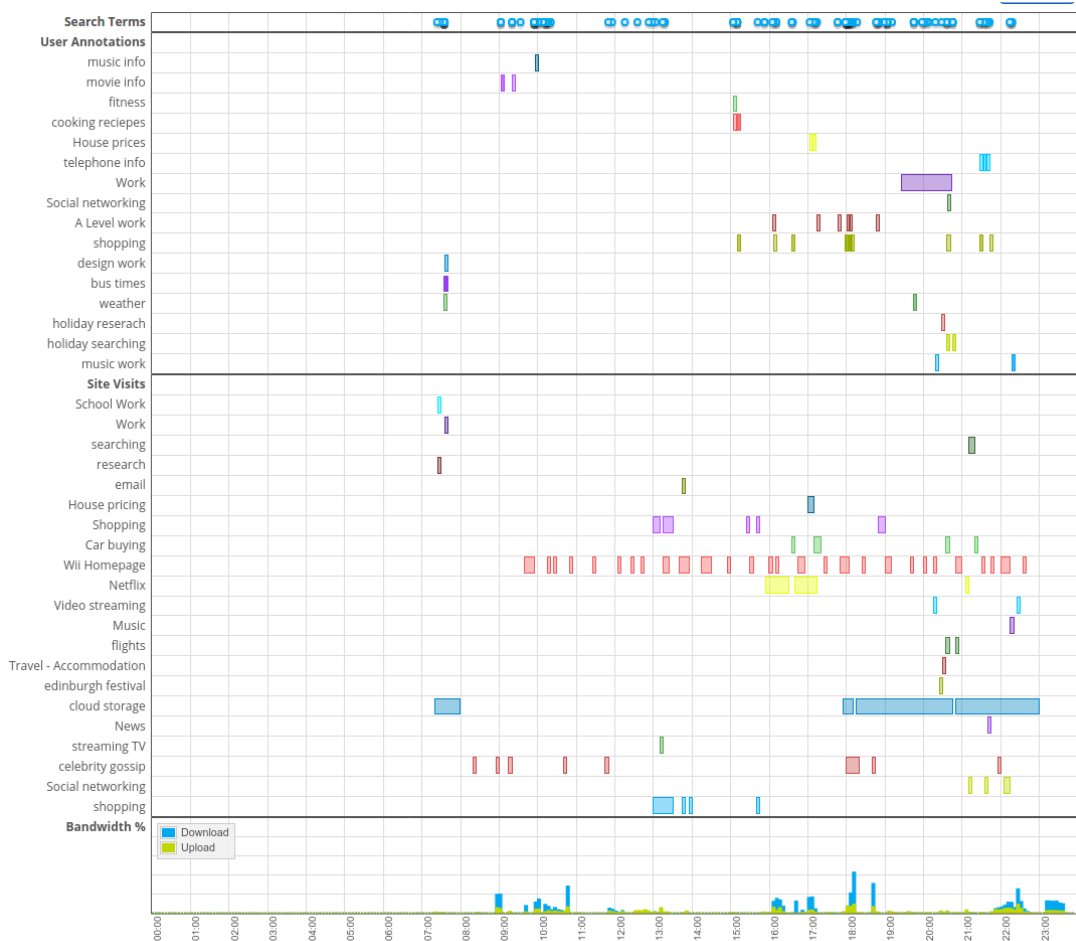


Figure 4.4: One day's annotated traffic combined (all devices) in household 1

ever, Household 1 did not provide any free activity annotations and Households 3 and 4 did not provide any Search activity or Search User annotations.

As the users added their annotations to the system the visualisation updated, an example of one days annotated traffic across all devices in Household 1 can be seen in Figure 4.4. One day's traffic for a single mobile device in Household 1 can be seen in Figure 4.5. Two interesting features can also be seen in Figure 4.5.

Firstly, marked with a red box and numbered 1 we can see a period of user activity (indicated by the presence of search terms) that has not been annotated. Second, marked with a red box and numbered 2 is an example of a social networking site appearing to be in use where there is no other activity that indicates

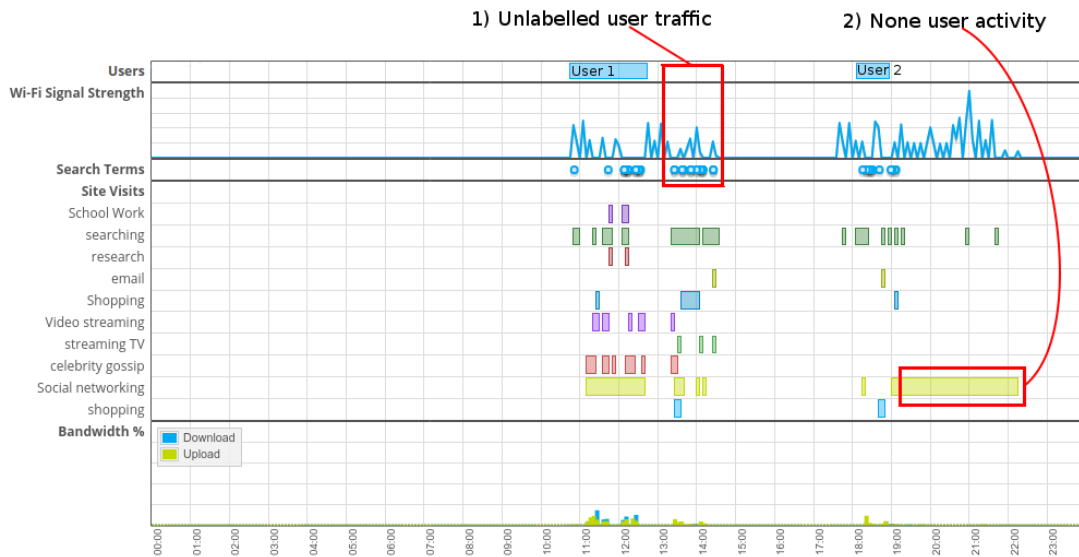


Figure 4.5: One day's annotated data for a shared device in household 1

that a user is present. This is an example of automated traffic caused by the polling behaviour of some modern web applications.

#### 4.3.4 Results: exit interviews

Exit interviews were performed at the end of the study and all participants were requested to be present. The interviews lasted about forty five minutes and where focused around five themes. The themes covered were: practicalities of the annotation process, utility of the annotated data, reactions to search term data, the language of annotation and finally privacy.

**Annotation practicalities.** When the participants were asked “who did the data annotation and how long did you spend completing the task?” the replies were similar across all the households:

**H1U1** “I did most of the annotation, and I found it very time consuming. I did it in batches ... 2 or 3 days at once ... when I had a bit of spare time. It was difficult to get anyone else to do it. They sometimes helped, but only if I asked them a question.”

---

**H2U2** “The tagging? I did all of it, it took me about 10-15 minutes each day.”

**H3U1** “It was me, I sometimes asked people if I was unsure what to put. I did it every couple of days and it took me less than half an hour to do.”

**H4U1** “We sat and did it together each evening. I’d say we spent about half an hour at a time.”

The next section of the interviews focused on what they liked and did not like about the annotation process. All of the households were unhappy with the amount of time it took to perform the task:

**H1U1** “It took way too long and I don’t think I would do it if it wasn’t part of this study.”

**H2U2** “I found it easy to add tags using the who and what buttons, but it still took too long”

**H3U1** “Tagging stuff was boring”

**H4U1** “It takes too long, and I don’t know what we would do with it anyway”

Feedback on the Host/Domain tagging interface was mixed:

**H1U1** “The site tags are good, I only needed to put them in once and it did the rest.”

**H2U2** “looking through the site was difficult, there were a lot in there, and I didn’t know what most of it was.”

**H4U2** “When tagging site, it was sometimes difficult to decide what to put. Some places[Web sites] have more than one use ... and going through the list was time-consuming.”

The mechanism for free user and activity tagging received positive feedback. Overall the participants stated that it was easy to use:

**H1U2** “The quickest way to do it[Annotation], was to look at the search terms and use the who tool to mark the who it was”



---

**H2U2** “I found it easy to add tags using the who and what buttons, but it still took too long”

From the above quotes it can be seen that one member of each household usually performed the annotation task, asking other family member for help when needed. Only Household 4 performed the annotation task together. All the households annotated the data in chunks when they had time and it took between 10 and 30 minutes a day. All households were unhappy with the amount of time it took to annotate the data.

The host/domain tagging interface was liked by Household 1 as it automatically tagged all traffic from that host/domain after it had been entered. However, Households 2 and 4 uncovered two problems. Firstly, there were a lot of unidentifiable host/domains in the data. These seemed to be caused by: the structure of modern websites (content delivery networks and third party tracking tools), software updates, and other background services running on the local host. This unidentifiable traffic made the task of adding host/domain tags time-consuming.

Secondly, HomeNetViewer assumed a one-to-one relationship between host/domain tags and activity and users. However, some host/domain tags have more than one legitimate use and different users use sites for different activities. This combined with the volume of traffic, particularly traffic that the users could not easily identify, added to the time it took to perform the annotation task.

**Utility of the annotated data.** To start discussion around the utility of the generated visualisations the participants were asked, “Thinking about the visualisations of the annotated data, can you tell me what you found useful?”. In response to this question all households made comments that highlighted improved visibility of activity on their networks:

**H1U1** “It offers a good overview of the usage, I didn’t know how much streaming H1U3 was doing. We have a 30 Gig cap on our package, so it could be a problem.”

**H2U2** “I was amazed by how much my phone talked to Facebook”

---

**H3U1** “Its shown me how much time I spend on eBay, I think I might have a bit of a problem! and I think H3U3 is watching far too much football on YouTube”

**H4U1** “Looking at the how little we use the Internet we should move to a cheaper provider.”

Household 3 also found the ability to monitor all their devices in one location useful.

**H3U1** “it’s similar to what I can see if I look at the browser history, which I do from time-to-time. To keep an eye on the kids ... this is easier though, because I can see it all in one place.”

One household suggested that the increased visibility offered by HomeNetViewer may lead them to rethink some of the house rules around the use of the Internet in bedrooms, stating:

**H3U1** “We don’t let the kids take computers and phones into their bedrooms. If they want to use the web they have to do it where we can keep an eye on them. Having this log of what has happened online might mean we could be a bit more flexible in future.”

Household 4 did not see any real use for the data. H4U2 said “It’s not that useful to us. I don’t need to know what [H4U1] is doing on the computer”. This point of view was also echoed by the younger participant H3U3 who said “Don’t see the point in it”.

To further prompt discussion around what could be seen in the annotated data the participants were asked, “Can you look at the data you have collected and tell me how it relates to your lifestyle?” The following discussions raised three observations. Firstly the routines of daily life were identifiable by the participants from the visualisations. They were able to see, and interpret, the ebb and flow of network activity caused by their household routines.

**H1U1** “You can see when [H1U2] gets home, there a lot more going on [the network].”

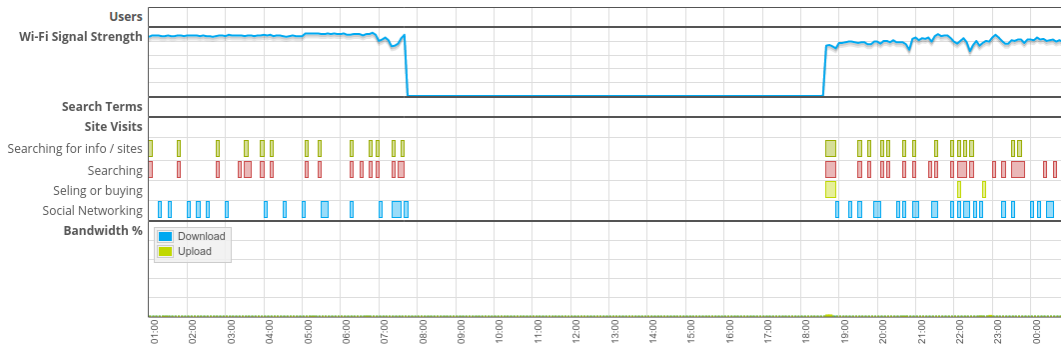


Figure 4.6: An example of the visibility of H2U4s’ daily routine and unknown traffic at odd times of night

**H2U4** “Look at my mobile, you can see when I left for work and when I came back. Have a look at H2U2’s mobile for me over a week, ... yeah you can see she leaves for work about 8:30 and gets back around 5 most days.” This can be seen in Figure 4.6.

The second observation was that automated traffic obscures true user activity. For example, users in Household 1, 2 and 4 were concerned about activity that they could not recognise at strange time of the night. An example of the mobile device that is mentioned below by H2U4 can be seen in Figure 4.6.

**H1U1** “This is my phone, but I don’t know why it is claiming to be in Facebook at 4am, That definitely was not me or anyone else at that time of the night!”

**H2U4** “I would like to know, for example, how often I used Facebook, but I can’t tell because of all the stuff that’s not me.”

**H4U2** “It looks like I was using my laptop on Saturday night, but I’m sure we were at a friends’ house.”

Finally, web browser behaviour and/or configuration can affect the accuracy of some annotations. The way in which the software used to access the World Wide Web has been configured can cause some incorrect annotations if Host/Domain tags are used. The first example of this was noticed by H1U2. They spotted an interesting discrepancy with the annotations relating to their iPad, “Look

---

there, that's been tagged as mum [H1U4], but I can see that was me". On closer inspection the tag for H1U4 had been derived from a Host/Domain user tags, after discussing it a bit more H1U4 realised that "the iPad goes to the sites you last had open [when you relaunch the web browser]".

Another occasion where this was seen in the user data was by H4U2 who commented, "hummm, it says I'm working a lot more than I would expect, it looks like I'm working every time I go on the computer". Closer inspection revealed that one of the sites that the user had tagged as "Work" was set to open when the browser was opened. This software/configuration specific behaviour reduces the accuracy of annotations.

Overall the reaction to the annotated data was positive. All households indicated that the visualisation had enabled them to gain new knowledge about what had happened on their networks. This shows that HomeNetViewer has achieved its main goal of improving network legibility. Another interesting finding is that users' routines are visible in the traces.

However, the annotation process is not perfect and there are two problems that affect the clarity and accuracy of the visualisation. Firstly, and most important is the presence of large amounts of automated traffic. This is traffic not related directly to user activity, but is caused by a number of automated processes. Second, some software used to access the Internet has unique and sometimes user configurable behaviour. This can cause the same network actions to be performed when they are used regardless of the user. This can lead to the automated user tags derived from host/domain data to be incorrect.

**The language of annotations.** One goal of this work was to assess the practicality of using users and activities as a vocabulary for annotating domestic network data. To encourage feedback in this area the participants were asked. "How did you feel about using activities and users to annotate your network data?" All the households indicated that they were comfortable using this type of language for this task.

**H1U1** "Most of the time it worked [using activities as tags]."

**H2U2** "Very practical, How else would you do it?"

---

**H4U2** “It felt fine, not difficult at all really.”

However, some participants indicated they had some problems using activities in some cases:

**H1U1** “It’s hard to know what to put sometimes, should I group Facebook and Twitter as Social Media or put them under their own tag?”

**H2U2** “I made a mistake early on putting google.com as Search, we use it for more than that.”

**H3U1** “I use Gmail for work, but H3U2 uses it for his private email his work email is somewhere else.”

The use of activities and users to annotate network data in domestic environments was positively received by all of the participating households. They indicated that using this type of language seems natural and often just worked. However, there are three difficulties in using this approach. Firstly, not all host/domains have a one-to-one mapping to user activity. Second, it is difficult at first to decide whether to use broad or precise language when adding an annotation. Finally, there is not always a simple relationship between activity and the sites being visited. This occurred for two reasons: not all users visit a given site for the same activity and some sites provide many different functions.

**Search term data.** To explore the utility of, and reaction to, search term data discussion was prompted with the question, “What do you think about the search term data, how did you use it?” The answers to this question were generally positive:

**H1U1** “Looking through the search terms is a bit embarrassing. There are loads of typos, but it makes it very easy to see what I was doing online.”

**H2U1** “They[search terms] are very useful, I often used them when adding tags to confirm what activity was taking place. I could also normally tell who the user was as well”

---

**H4U2** “I like the search data, it’s a bit like a diary. I can look back and see what I was searching for, which tells me what I was doing.”

However, most of the households also raised concerns over the intrusive nature of the search term data. Most users were uncomfortable with the level of information exposed by search terms. The comments regarding this are dealt with next, alongside the other privacy related concerns.

**Privacy.** The previous question on dealing with search terms led the users into a discussion on the privacy related issues of HomeNetViewer. This discussion was further encouraged by asking, “How did you feel about the extra information HomeNetViewer makes visible to the rest of the household?” Generally the reactions were positive or indifferent towards most of the data exposed by HomeNetViewer:

**H1U1** “The sites and activity is[sic] fine. It’s pretty general.”

**H2U1** “I’m happy for the family to see that data. I would not want anyone else to see it though”

**H3U2** “I didn’t mind people seeing which sites I visited. It’s like looking at the browser history.”

**H4U1** “It’s OK, I’m not sure I would look at it if I’m being totally honest.”

However, the search term data proved controversial in all but one household. This shows some discomfort with the level of information they expose:

**H2U3** “I don’t like these[search term data], I don’t mind people knowing I’m Googling ... but I might be looking up something private”

**H3U2** “The search terms give too much away.”

Another interesting point raised in one household was how HomeNetViewer installation caused discussions around acceptable behaviour on the domestic network:

---

**H2U1** “Just after you installed it [HomeNetViewer], H2U2 had a chat with me about what I thought was acceptable ... not that she was doing anything wrong, she just wanted to make sure.”

This comment is important because it highlights two things. Firstly, the interaction between the visibility of network activities and the negotiation of domestic network policy. Second, this indicates that some users may have altered their behaviour once they became aware of the level of transparency HomeNetViewer offered.

## 4.4 Discussion

All the participants were able to understand the interactive time-line visualisation, with little or no training. Additionally, all households provided feedback demonstrating that they were able to gain new insight into their network usage. This indicates that the interactive time-line visualisations are beneficial and improved domestic network legibility.

HomeNetViewer also shows that it is possible for users to annotate their own data and that these annotations help to enhance understanding of their network usage. The combination of interactive time-line visualisation and user contributed annotations to create user-centred presentations of network activity can be a valuable tool for increasing network legibility and supporting self-management of domestic networks. There were several other positive findings from the deployment of HomeNetViewer.

All of the users in the deployment are comfortable using activities and users as a vocabulary for annotating domestic network data. This supports the findings of Brundell et al. [18]. However, the deliberately unrestricted text entry implemented in this version of HomeNetViewer caused some frustration. Participants found it difficult to chose the correct scope of the annotation for some hosts/domains.

All of the participants were comfortable working with host/domain data extracted from HTTP/S traffic. The host names and domain names of interest were identifiable in the list of all visited sites. However, a large number of unknown

---

hosts/domains were present in the interfaces. These unknown hosts/domains caused frustration for the participants. The initial design work highlighted this issues with advertising related traffic. In spite of efforts to filter this out, they were not 100% effective.

In the final dataset the most prevalent cause of unknown domains related to the structure of modern web applications. Modern web applications often use load balancing, content delivery networks, and third party hosted content to enhance the performance of their applications. This can lead to a large number of unidentifiable host/domains being listed that appear to be unconnected to the original site accessed.

A further issue highlighted by the participants related to host/domain annotation, is that some host/domains support multiple activities. The deployed version of HomeNetViewer only allowed one host/domain annotation per host/domain to be entered. Allowing multiple annotations per host/domain would be trivial in the interface, but would cause difficulties in the visualisation. How would the system choose the correct annotation to display back to the user? One household also noticed that some hosts/domains mapped to different activities for different users. How best to deal with these complexities is left as an open question for future exploration.

The final aspect to discuss is that of respecting privacy and the use of search term data. The participants in the study were generally happy with other members of their household seeing a history of websites they have visited. However, this was a small sample which may have been skewed to more open households. A number of households who initially showed an interest in taking part in the study, declined to participate when they were given more information on the type of data collected and made visible to the rest of the household. This shows that concerns about privacy vary between households. Addressing this privacy issue for a broader population would be a key challenge in taking this type of technology further.

Search term data were also controversial among the participants. Search term data were found to be an effective way for participants to identify activities and users on their networks. They acted as: reminders of events, clues to activities and clues to users. They were also used extensively by participants to perform the



---

annotation process. Search terms are a valuable source of information that can be used to contextualise network traffic. However, they were deemed intrusive by many participants as they gave away too much information to the rest of the household. Most of the privacy related discussions in the exit interviews focused on the issues surrounding information exposed by search term data.

Overall the HomeNetViewer platform enabled users to gain new insights into the traffic on their domestic networks. However, there is room for improvement and several open challenges remain.

The main complaint made by the participants concerned the time taken to perform the manual annotation task. Reducing the time taken to annotate the data would be worth investigating in future. The annotation task itself was time consuming. Having to examine the each device on the network in turn and look through periods of high activity was tedious. A number of participants noted that the unidentifiable traffic in the interfaces also slowed down the annotation process.

The HomeNetViewer system removed a significant proportion of advertising traffic using domain blacklisting, in an attempt to remove unknown hosts/domains from the interface. Unfortunately, this was not 100% effective as some advertising related traffic was still visible in the annotation interfaces. Another source of automated traffic observed was from software and operating system updates. This type of automated traffic was seen on most types of devices.

The traffic caused by software and operating system updates did not adversely affect the visualisations, because users chose not to annotate this type of traffic. It did, however, clutter the annotation interfaces. The design and implementation practices of modern web applications also contributed to the high levels of unknown host/domains in the annotation interfaces. How to reduce the impact of these factors on manual data annotation remains unresolved.

The polling behaviours of modern web applications and mobile phone apps caused some annoyance and frustration to the users in the study when combined with host/domain annotations. Websites and apps like Facebook, Twitter and many more exhibit this type of behaviour, which leads to sites being reported as in-use even if the user was not actively using the device. The ability to distinguish between user generated and automated polling for updates would be beneficial

---

to the understanding of the visualisations and reduce the amount of unknown hosts/domains in the annotation interfaces.

The last aspect worth discussing were the technical problems encountered during the deployment of HomeNetViewer. Most devices worked well with HomeNetViewer and after installation no households reported any problems. However, a number of devices encountered during the installation had problems with transparent SSL proxies “in the wild”. These devices fell into three categories,

The first set of devices did not respect the certificates in the devices key store for certain apps. For example, Android phones did not use the device key store when accessing Google services such as the Google Play store. The Apple iPhone had similar restrictions in place for accessing the Apple app store and a number of banking applications were also affected. These restrictions stopped the participants from installing new apps on their mobile devices or using specific applications while connected to the HomeNetViewer enabled router. These restrictions were likely put in-place by the App developers to stop MITM attacks on the SSL traffic as they contain sensitive information.

The second set of devices did not offer a way to configure the internal device keychain and were unable to be configured to accept HomeNetViewer’s SSL certificate. These were all consumer grade devices, designed for accessing media over the Internet. For example, Roku media streamer. These devices still provided useful information as HomeNetViewer was designed to cache the forward DNS lookup, which enabled the IP addresses in the HTTPS headers to be converted to relevant hostnames, which were then displayed to the users in the interface.

The third and final class of devices had some form of proxy detection to prevent the caching of the data they receive. These included the Sky+HD receiver, Sky Now TV box, and the PlayStation 4. These devices refused to function when the Squid proxy was enabled. There was no option other than to exclude these devices from the study. This was achieved by reconnecting them back to the households original router so they would remain functional. This meant that no data were collected from these devices.

The above problems show that using a transparent HTTP/S proxy with SSL interception is not currently a viable option for deploying this type of system in domestic environments. This means the extraction of full URLs and search term

---

data is not practical for deployment in real environments. Interestingly, this may help with debate surrounding the use of search term data, but it also removes a useful source of information used in the annotation process. How removing search term data would affect both these issues would require further investigation. Next we discuss the limitations of this work.

## 4.5 Limitations

Recruiting participants for this study was particularly difficult. This is reflected in the small number of deployments. While every effort was made to recruit a wide range of households it was not possible to find a single person or multiple occupancy household, for example, a student house or house of young professionals to include. Multiple occupancy households would have been of particular interest as it has been reported that sharing Internet connections in these environments can cause tension between the house-mates [20]. It would have also be interesting to see if there were differences in the privacy sensitivity between family and multiple occupancy households.

Related to the difficulty in recruiting participants is the possibility of introducing self-selection bias. It was only possible to recruit households who were happy for all members of the household to have access to each others' online activity. Hence, the families that volunteered are likely to have a more relaxed attitude to their online privacy within the family unit than the general population.

Another limitation to consider is whether the increased visibility provided by HomeNetViewer have caused the participants to alter their behaviour. Household 1 reported a conversation regarding "what was deemed acceptable behaviour" shortly after HomeNetviewer was installed. It is unclear which activities, or by how much, the participants may have modified their behaviour and so it is difficult to estimate its impact, if any, on the results. If behaviour change did occur it is likely that it was in a small number of activities deemed unacceptable by that particular family. Hence, we hypothesise this effect will not significantly impact the data collected as the majority of online activities do not fall into this category.

It was also not possible to collect all data from all devices in the participating households due to the incompatibility of some devices with the transparent Squid

---

proxy and SSL bump module. A number of media devices and games consoles had to be removed from the deployments. Hence, we did not capture representative traffic from these device types.

The exit interviews were performed as a household group. It therefore was difficult to engage all the participants. The younger participants presented particular difficulties as they seemed unwilling to speak openly while their parents were present. This may have led to the feedback from participants being skewed to the views of the adults in some households.

The deployment of HomeNetViewer has shown that user-centred presentations of domestic network data are useful domestic to users and increases domestic network legibility. It has also raised some interesting challenges. The main issue raised by the participants was the time taken to perform the manual annotation of the data. The next section of this dissertation looks at using enterprise traffic classification techniques to reduce the annotation burden.

## Chapter 5

# Automatic generation of user-centred presentations of network activity from IP Flow records

The deployment of HomeNetViewer, described in Chapter 4, highlights the need to reduce the annotation burden on users. In this chapter, one approach to reduce the annotation burden is explored.

A number of possible approaches to this problem are highlighted in section 2.6 of the literature review. Due to the recent move towards HTTPS as the default protocol, and the difficulty in deploying a transparent SSL proxy in the home, methods that require deep packet inspection are ruled out. Hence, enterprise traffic classification techniques that use IP Flow records as the feature vectors are considered. These have been shown to be effective in classifying traffic in commercial environments to improve network legibility for networking professionals. Enterprise traffic classification techniques work by automatically grouping traffic into classes based on the statistical properties of the IP Flows. The classes used in enterprise traffic classification are based around network protocol. This is different to the classes in the HomeNetViewer dataset [18]. Each class in the HomeNetViewer dataset contains traffic from a number of protocols and there

---

is no direct relationship between class and protocol. This chapter explores the following question:

**Q4.0** Can enterprise traffic classification techniques be used with user contributed annotations to automatically annotate domestic network traffic?

The data collected in Chapter 4 enables the generation of an annotated IP Flow dataset. Using this it is possible to formulate two multi-class classification problems, similar to those described in the traffic classification literature. In the first case, the target classes are the users and the input features are the data contained within the IP Flow records. In the second case, the target classes are the activities and the input features are the data contained within the IP Flow records.

The rest of this chapter focuses on the analysis of the HomeNetViewer dataset. This dataset is used to assess the viability of enterprise traffic classification techniques in domestic environments. The performance of various classifiers and the importance of the available feature vectors are explored. Next, the important terms are defined.

## 5.1 Performance metrics

The performance of machine learning classifiers is typically quantified using the standard metrics: precision, recall, and F1-measure [12]. To understand these metrics it is first important to define four terms:

**True Positive** measures the number of positives that are correctly identified as positives.

**True Negative** measures the number of negatives that are correctly identified as negatives.

**False Positive** measures the number of negatives that are incorrectly identified as positives.

**False Negative** measures the number of positives that are incorrectly identified as negatives.

---

In the literature these are also commonly discussed in terms of type I and type II errors. These are defined as:

**Type I** is the incorrect rejection of a true null hypothesis, equivalent to a false positive.

**Type II** is failure to reject a false null hypothesis, equivalent to a false negative.

Now that the basic terminology has been defined, the performance metrics used in this chapter can be defined.

**Precision:** for a particular class, this is defined as the ratio of True Positives to the sum of the True Negatives and False Positives, see 5.1.

$$Precision = \frac{TruePositives}{(TrueNegatives + FalsePositives)} \quad (5.1)$$

The closer the value is to one, the lower the number of type I errors committed by the classifier.

**Recall:** for a particular class, this is defined as the ratio of True Positives to the sum of the True Positives and False Negatives, shown in 5.2

$$Recall = \frac{TruePositives}{(TruePositives + FalseNegatives)} \quad (5.2)$$

The closer the value is to one, the lower the number of type II errors are committed by the classifier.

**F1-measure:** this weights both precision and recall into one metric, by taking their harmonic mean, shown in 5.3.

$$F1 - measure = 2 \left( \frac{Precision * Recall}{Precision + Recall} \right) \quad (5.3)$$

Higher values of F1-measure indicate better overall classifier performance.

In this chapter the results are presented per-class using the above metrics for both user and activity classification tasks. When presenting the Precision,

---

Recall, and F1-measure the support values are also provided. This is defined as: the number of occurrences of each class labelled in the validation dataset.

Alongside these numerical values a normalised confusion matrix is also displayed. The confusion matrix visualises classification errors. A normalised confusion matrix is used to account for the differing number of members of each class. Next, the HomeNetViewer dataset is described including its feature vectors and target classes.

## 5.2 Dataset and classes

The dataset used in this work is taken from the deployment of HomeNetViewer in 4 real UK households. Details of the deployment and data collection can be seen in Chapter 4. An IP flow is defined as “a set of IP packets passing an Observation Point in the network during a certain time interval. All packets belonging to a particular Flow have a set of common properties.” [21]. In this dataset, the Observation Point is the household Access Point. An IP flow in its most basic form is described as a tuple containing: the source and destination IP address, source and destination ports, protocol type and duration. However, it can be augmented with any number of other properties, for example, packet inter-arrival time or payload size Moore et al. identify 249 possibilities [60]. The structure of the data collected by the HomeNetViewer platform is shown in Table 5.1.

The data were not collected or annotated with the intention of testing enterprise traffic classification techniques. Hence, the full headers of each packet were not collected. This limits the analysis, as the raw data are not available to calculate many of the feature vectors suggested by Moore et al. [60]. Therefore, the analysis is limited to the data collected by the HomeNetViewer platform. Irrespective of this, the data collected contain enough information for basic analysis. The annotations used to generate the ground truth are provided by real users, making this a reasonably realistic scenario.

Before the data analysis could be performed the IP Flow data had to be processed through the following four steps. Firstly, the appropriate flows had to be selected from the HomeNetViewer database. IP Flows on all ports were



---

Field	Description
macaddr	MAC address of the local device
dir	The flow direction
proto	The flows protocol type
saddr	The IP address of the source
sport	The port for the source
daddr	The IP address of the destination
dport	The port for the destination
npkts	The number of packets in the flow
nbytes	The number of bytes sent through the flow
startTime	The time the IP Flow started in ms since the Unix epoch
endTime	The time the IP Flow ended in ms
duration	Length of flow in ms

Table 5.1: Description of the Flow data collected

selected between the start and end of the three week deployment. All IP Flows going between hosts on the local network were excluded from the dataset.

Second, three new compound features were calculated for each flow. Each one is described in turn below.

**Flow delta** is the elapsed time since an IP Flow on the same port from the same source and destination was seen on a particular device. The feature was created to capture the timing between similar events. The time between events may vary due to user routines/characteristics, activity characteristics and the type of data being delivered.

**Packet rate** is defined as the number of packets in an IP Flow divided by the length in seconds of the IP Flow. This feature was selected as it may show activity specific properties, for example, the difference between video streaming and web browsing.

**Average packet bytes** is defined as the total number of bytes sent through an IP Flow divided by the number of packets in the IP Flow. This feature was calculated as it may highlight the difference between some activities, for example, video streaming or audio streaming.

---

In the third step, the user generated annotations are used to attach ground truth to each IP Flow in the dataset. Each annotation contains the MAC address of a device and a time-stamp of the start and end of the annotation. Assigning ground truth was achieved by iterating through all the flows and looking for an annotation that has a matching MAC address and a start time-stamp, between the start and end time of the annotation. Any IP Flow that did not meet this criteria was assigned to the Unknown class. This process was performed twice for each household. Once for the user annotations and once for the activity annotations. This generates two datasets per household.

The fourth, and final step, was to split the datasets for each household into a training and validation set. Data from the first week was used as the training set and the final two weeks were used as the validation set. The following naming convention is used when referring to datasets: Household [1:4], annotation type[U,A], data type [T,V]. For example, H1AV is the verification set for Household one's activity annotations and H3UT is Household three's user annotation training set.

### 5.3 Classification algorithm and feature selection

A number of classification algorithms are commonly used for enterprise traffic classification, see section 2.6. Recent work in fine-grained traffic classification focusing on HTTP/S traffic has shown decision tree based Random Forest classifiers perform well on IP Flow data [36]. However, this work focuses on an enterprise focused set of target classes. Each algorithm also has its own strengths and weaknesses, depending on the properties of the dataset. Therefore, to achieve best performance it is important to test, and select, the algorithm most appropriate for the problem. In this section the performance of five classification algorithms are tested: k-Nearest Neighbours (K-NN), Gaussian Naive Bayes (GNB), Multinomial Naive Bayes (MNB), Decision tree (DT) and Random Forest (RF) and Support Vector Machines (SVM). All algorithms used were provided by the Scikit-learn toolkit in python [66].

---

The  $k$ -fold cross-validation methodology is used to estimate the performance of each classifier.  $k$ -fold cross-validation take the training dataset and splits it into  $k$  chunks, or folds. Each fold is then used as a validation set once, with the remaining  $k - 1$  folds used to create a training set.

$k$ -fold cross-validation is often used to estimate classifier performance, as it eliminates bias introduced through the selection of the training and validation datasets [48]. The number of folds used in this experiment was ten.

For each algorithm it is also important to select the correct set of features to optimise performance. As only ten features are available all are exhaustively tested. The features were ranked using the ANOVA F-value statistic, which measures the dependency between the feature and the classes.

Before the algorithms were tested the data were pre-processed. Two processes were applied. Firstly, all non-numeric features were converted to numerical values. This is important as not all classifiers can handle non-numeric data. The features converted in this dataset were MAC address and IP address that were converted to their respective integer forms. Second, scaling was applied to all features. The scaling stops the wide range of values in raw data skewing the results of the objective functions.

For each classification algorithm a  $k$ -fold cross-validation was performed on the H1UT and H1AT datasets for each classifier with the features added one-by-one in rank order, according to the ANOVA F-value. The results for the user classification and activity classification can be seen in Figures 5.1 and 5.2 respectively.

It can be seen in Figures 5.1 and 5.2 that the tree based classifiers perform best on both datasets, supporting the findings of Grimaudo et al. [36]. The SVM classifier required CPU and memory capacity beyond those available, due to the large number of data points and classes. It did not finish within 24 hours, so it was excluded. Classifiers that rely on the underlying statistical properties of the data, such as, GNB and MNB, performed poorly in both classification tasks. Hence, the Random Forest classifier was chosen to complete the final data analysis.

Figures 5.1 and 5.2 also show the impact of each feature vector on the classifier performance. It can be seen, in both cases, that the performance of the Random

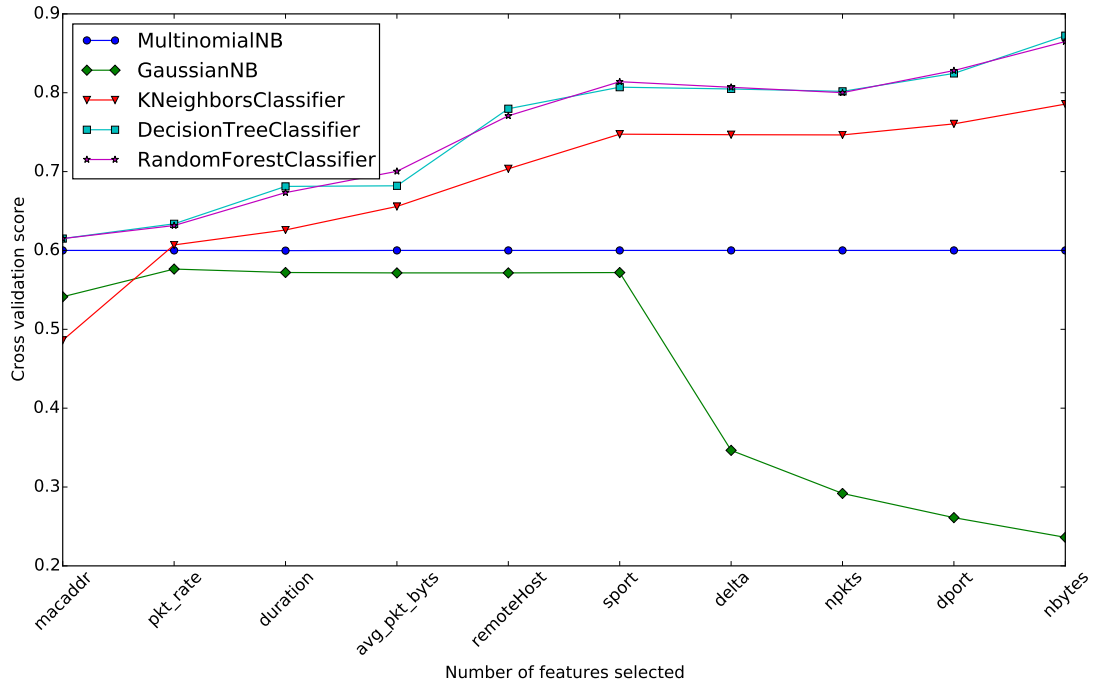


Figure 5.1: Classifier performance H1UT dataset

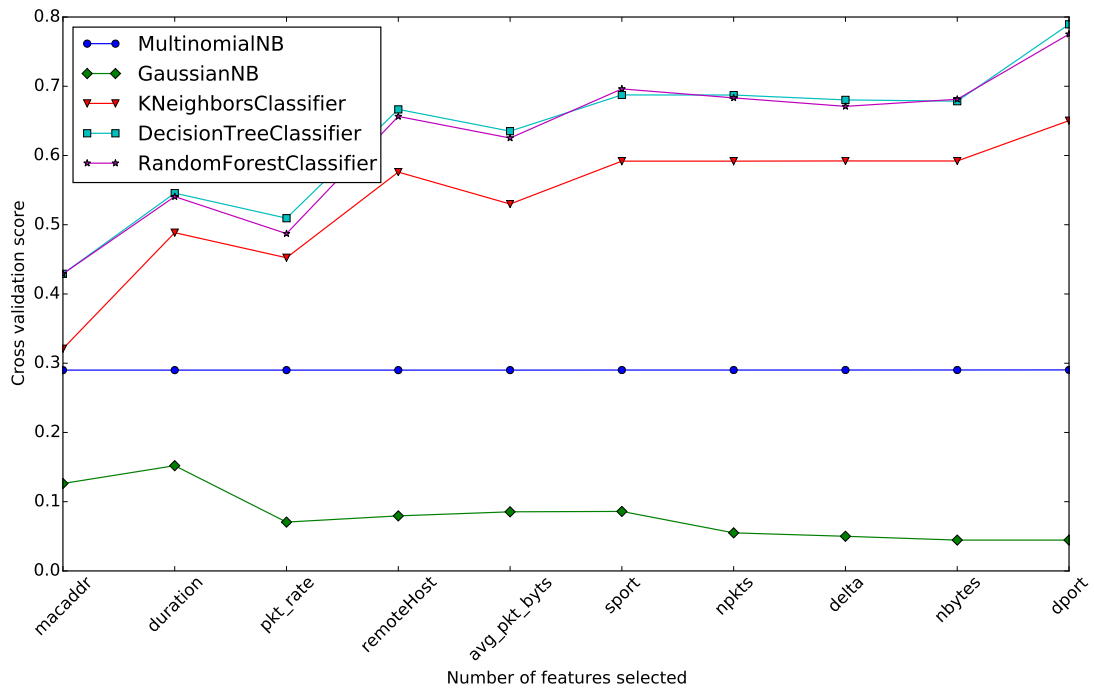


Figure 5.2: Classifier performance H1AT dataset

---

Forest classifier increases steadily until the sixth feature is added. After that the improvement begins to level off. For this reason, only the best six features are considered for the rest of the analysis.

After the selection of the Random Forest classifier and the six best features, the available parameters can now be optimised. The Scikit-learn implementation has two parameters that are related to the accuracy of the resulting classifier. The first is the number of *estimators*, which is the maximum number of trees in the forest. The second is the *criterion*, used to measure the quality of the split at each branch. Scikit-learn offers two criteria, Gini impurity and entropy. Gini impurity is a measure of how frequently a randomly selected element from the data would be incorrectly labelled if it were randomly labelled according to the distribution of labels in the data. Entropy is information gain. Figures 5.3 and 5.4 show the results of a grid search of these parameters used to find their optimal values.

The graphs show, in both user and activity classification, that the entropy split criterion out performs Gini impurity. In the user classification task, classifier performance improves up to 100 estimators and then levels off. In the activity classification task, classifier performance improves up to 60 estimators and then levels off. Therefore, 100 and 60 were used as the number of estimators for the user and activity classifiers respectively.

After finding the best performing classifier and optimising its parameters on the H1UT and H1AT datasets, the next step is to assess the performance of the classifier on all the data collected from each household, using training sets to train the classifier and the verification set to assess its performance. The results of this process are presented in the next section.

## 5.4 Results

This section presents the results generated by testing the Random Forest classifier. Using the parameters found in the previous section for both the user and activity recognition tasks. These results were obtained by training the classifier on the first week's data for each household. The remaining two weeks' data are then used to assess classification performance. For the user classification task a full

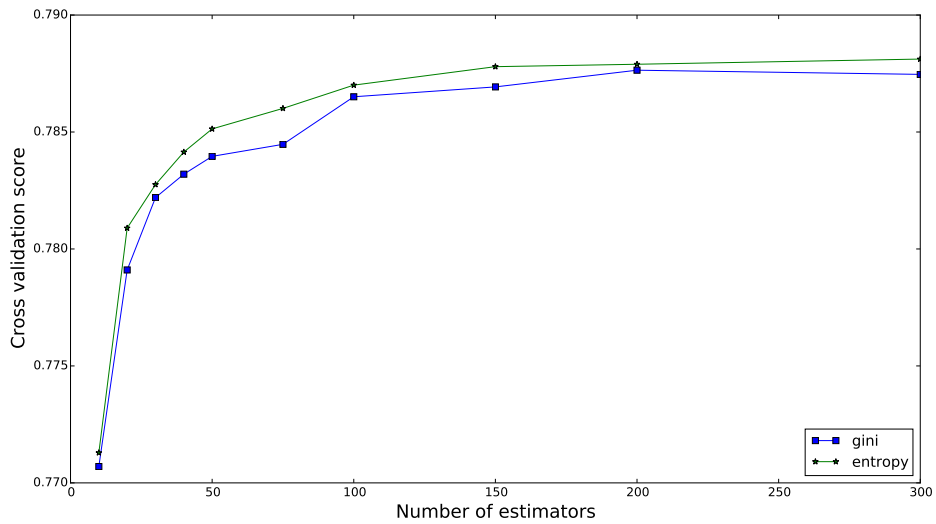


Figure 5.3: Classifier performance H1UT dataset with increasing number of estimators

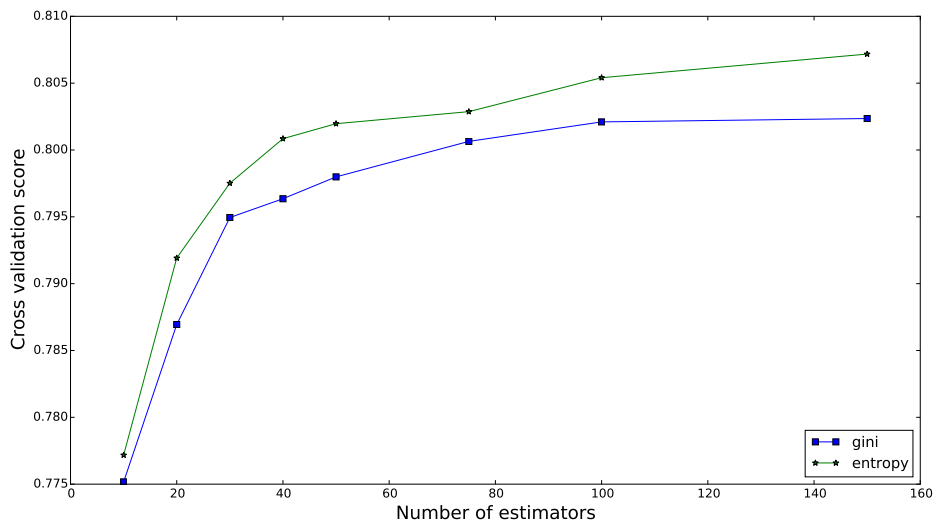


Figure 5.4: Classifier performance H1AT dataset with increasing number of estimators

---

set of precision, recall and F1-measure, and confusion matrices are provided. For the activity classification task, the same metrics are presented on a subset of the available classes. Since not all activity classes have examples in the training and verification datasets, calculating the required metrics is impossible.

Before going further it is worth discussing one important feature of the dataset: the presence of unlabelled data. The annotation process used in HomeNetViewer leads to a large proportion, approximately 50%, of the data being unlabelled. These data are assigned to the Unknown class. Within the Unknown class there will be a mix of traffic. Some will be unrelated to users and activities. However, the annotation method is not 100% accurate. Users are fallible, and all not all user traffic has been annotated. An example of this can be seen in Figure 4.4.

Therefore, the traffic labelled as Unknown will contain a mix of user and none user traffic. This is important to consider when reviewing the results presented below. The metrics used will treat any flow with an Unknown label that is classified as user traffic, to be a false positive. Unfortunately this is not the always the case, because the annotation method is not 100% accurate. This effectively increases the number of false positives reducing the reported precision value and consequently the F1-measure.

No realistic way to compensate for this issue could be found. Therefore, two values for the precision and F-measure are calculated. The pessimistic/standard value that underestimates classifier performance and an optimistic values that over estimates classifier performance. The optimistic values are calculated by treating false positives with the Unknown class as true positives. These values provide a range, within which, the true value lies. Both values are displayed in the tables. The pessimistic/standard value is shown first, with the optimistic value in brackets.

---

### 5.4.1 Household 1

	precision	recall	f1-measure	support
Unknown	0.52	0.73	0.60	208219
user 1	0.42 (0.79)	0.55	0.48 (0.65)	32249
user 2	0.48 (0.81)	0.29	0.36 (0.43)	92197
user 3	0.08 (0.48)	0.03	0.05 (0.6)	23795
user 4	0.36 (0.84)	0.10	0.15 (0.18)	57815
avg / total	0.46 (0.73)	0.49	0.45 (0.59)	414275

Table 5.2: H1UV classification results, optimistic precision shown in ( )

	precision	recall	f1-measure	support
cloud storage	0.83	0.60	0.69	18892
cooking reciepes[sic]	0.00	0.00	0.00	254
design work	0.00	0.00	0.00	6
email	0.00	0.00	0.00	44
fitness	0.00	0.00	0.00	6
leisure	0.24	0.02	0.04	8540
leisure info	0.91	0.59	0.72	32660
movie info	0.00	0.00	0.00	24
music info	0.00	0.00	0.00	39144
music work	0.01	0.01	0.01	110
school work	0.00	0.00	0.00	384
shopping	0.01	0.04	0.01	2114
social networking	0.00	0.23	0.00	194
Unknown	0.23	0.33	0.27	7960
web searching	0.98	0.01	0.03	65234
work	0.00	0.00	0.00	12

Table 5.3: H1AV classification results

**User Classification** results for Household 1 are shown in 5.2. It can be seen that the classifier has mixed performance. For user 1 the classifier performs well with F-measures between 0.48 and 0.65. However, for users 2, 3, and 4 the classifier performs much worse achieving F1-measures below 0.43. The recall for users 3 and 4 is also very low. This means that most of the traffic in the verification set for users 3 and 4 was missed by the classifier. The confusion



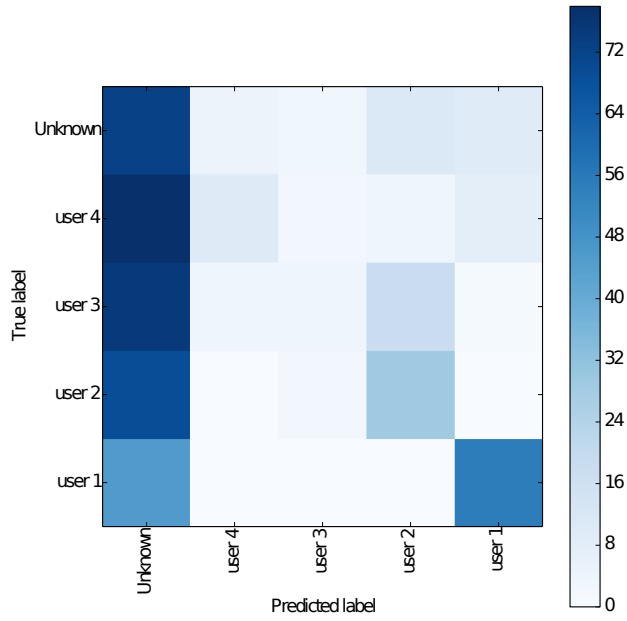


Figure 5.5: H1UV confusion matrix

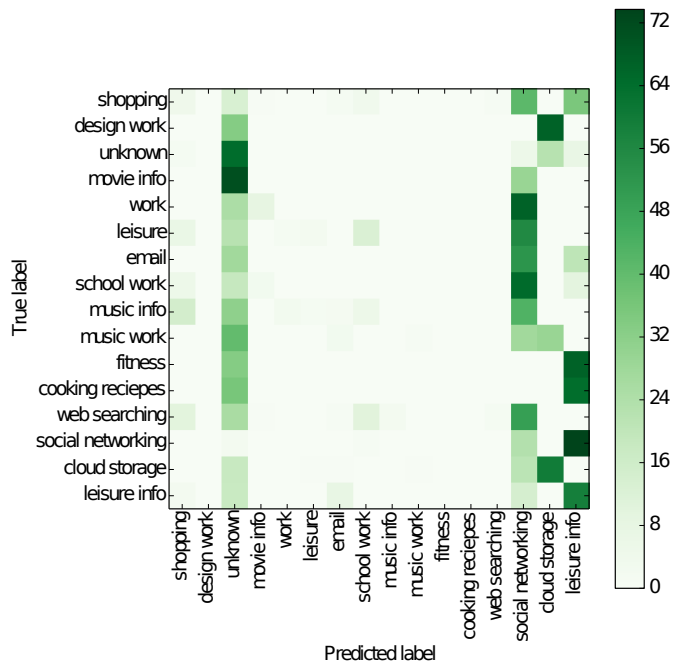


Figure 5.6: H1AV confusion matrix

---

matrix in Figure 5.5 shows that for users 1 and 2 there is little or no confusion between traffic from other users, only in the Unknown class. However, for user 3 and 4 there is visible confusion between them and other users.

**Activity classification** for Household 1 is disappointing, almost all the activities are not correctly classified by the classifier. For the classes that do report some correct classification (cloud storage, leisure, leisure info, social networking, and web searching) the confusion matrix in Figure 5.6 shows that there is widespread confusion between the classes. However, three of the classes show interesting features:

**social networking** is confused with almost all other classes. There are two possible explanations for this. Firstly, social media sites are pervasive on the web, and are often integrated into other site using “Like and share” buttons. Second, social media sites when open in a browser, or an App is installed on a device, will periodically poll for new updates. This periodic polling occurs in the background of other activities. Hence, social media traffic may have been mislabelled. It is possible that both of these features contribute to the confusion of the “social networking” class.

**cloud storage** is often confused with the “design work” and “music work” classes. It is possible that the use of a cloud storage service is related to the “design work” and “music work” activities, for sharing files with colleagues or storage of backups.

**music info** is not detected by the classifier at all in the H1AV data set, in spite of the high support value. Closer inspection of the raw data reveals that the sites annotated in the training set as “music info” are different to the sites labelled in the verification set. This indicates that the training set has not captured all the user behaviour.

## 5.4.2 Household 2

**User Classification** in Household 2 was complicated by the return of user 2 from university after the first week of the study had elapsed. This means that user 2 has no data in the H2UT dataset. It was decided to leave the data for user

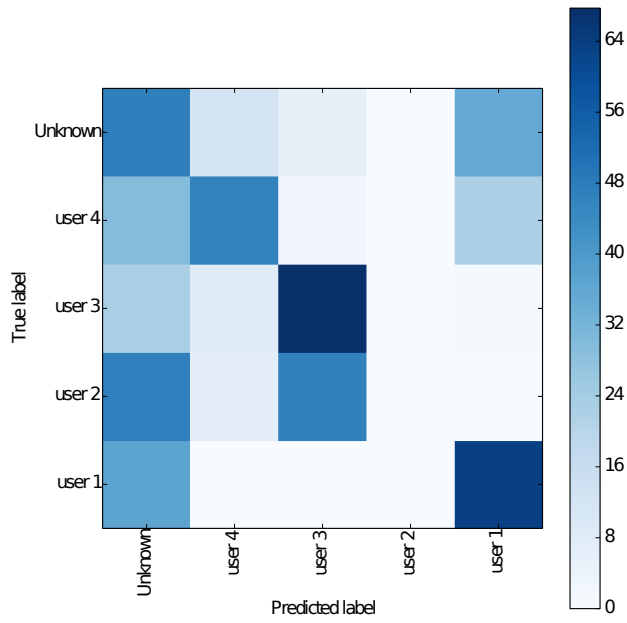


Figure 5.7: H2UV confusion matrix

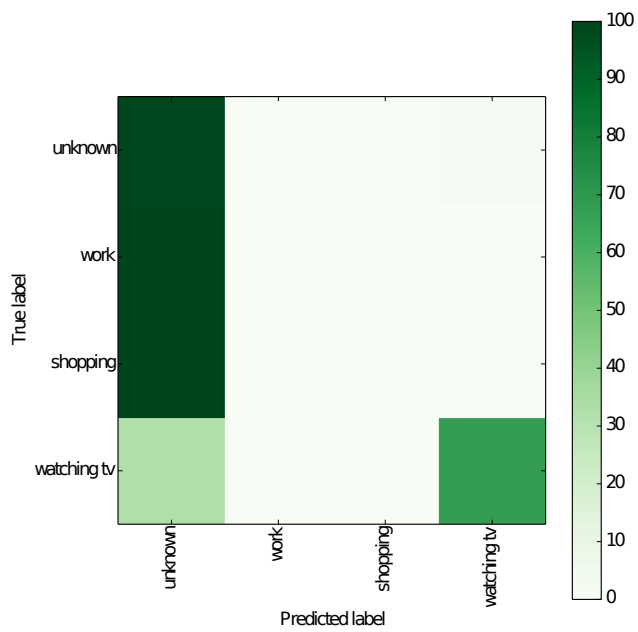


Figure 5.8: H2AV confusion matrix

---

	precision	recall	f1-measure	support
Unknown	0.28	0.47	0.35	42699
user 1	0.68 (0.93)	0.63	0.66 (0.75)	61838
user 2	0.00 (0.00)	0.00	0.00 (0.00)	39470
user 3	0.51 (0.57)	0.68	0.58 (0.62)	31793
user 4	0.35 (0.49)	0.46	0.40 (0.47)	12085
avg / total	0.40 (0.50)	0.46	0.42 (0.48)	187885

Table 5.4: H2UV classification results, optimistic precision shown in ()

	<b>precision</b>	<b>recall</b>	<b>f1-measure</b>	<b>support</b>
shopping	0.55	0.00	0.00	6231
Unknown	0.08	0.00	0.00	26916
watching tv	0.63	0.68	0.65	3523
work	0.00	0.00	0.00	361

Table 5.5: H2AV classification results

2 in the dataset to see how data from a new user joining the network affects the classifier. As expected user 2 is never correctly identified by the classifier and is misclassified as user 3 and user 4. This highlights that the social make-up of the household is dynamic and changing, and these changes can affect classification accuracy. The remaining users in the household were well classified. User 1 was only ever confused with traffic in the Unknown class with a precision between 68% and 93%. The confusion matrix in Figure 5.7 show there is some confusion between user 3 and user 2, and user 4 and user 1.

**Activity classification** results for household 2 are disappointing. Only one class, watching TV, achieved a positive F-1 measure. The recall values of zero (two decimal places) for shopping and work are due to a large number of False Negatives, i.e. examples that were missed by the classifier. This shows that the classifier could not properly identify examples from those classes in the validation set. This could be for two possible reasons. Firstly, the examples in the training set are not representative of the examples in the validation set. For example, the shopping that was labelled in the training occurred on site A and the shopping in labelled verification set occurred on site B. The second explanation is that the feature vectors do not provide enough information to distinguish between the

---

classes. However, where the classifier was able to correctly identify the activity, watching TV, there was no confusion except with the Unknown class.

### 5.4.3 Household 3

	precision	recall	f1-measure	support
Unknown	0.81	0.66	0.73	145001
user 1	0.60 (0.97)	0.90	0.72 (0.93)	79469
user 2	0.80 (0.99)	0.33	0.47 (0.49)	17376
user 3	0.76 (0.97)	0.51	0.61 (0.67)	12492
avg / total	0.74 (0.98)	0.71	0.70 (0.82)	254338

Table 5.6: H3UV classification results, optimistic precision shown in ()

	precision	recall	f1-measure	support
football	0.42	0.58	0.49	21478
gaming	0.16	0.35	0.22	4740
organising day out	0.01	0.45	0.02	757
selling items	0.41	0.62	0.50	39387
Unknown	0.43	0.53	0.47	7101

Table 5.7: H3AV classification results

**User Classifications** for Household 3 provides the best results for the user classification task. This is indicated by the presence of a strong diagonal in Figure 5.9 and the high average F1-measure between (0.70 and 0.82) in Table 5.6. It can be seen from Figure 5.9 that there is a small amount confusion between user 3 and user 1.

**Activity classification** in Household 3 was the best in the group with two classes with F1-measures approaching 0.5. However, there is still significant confusion between all classes.

### 5.4.4 Household 4

**User Classification** in Household 4 is disappointing given that it has only two classes. It can be seen in Figure 5.11 that Users 1 and 2 are not often confused. However, there is significant confusion with the Unknown class.

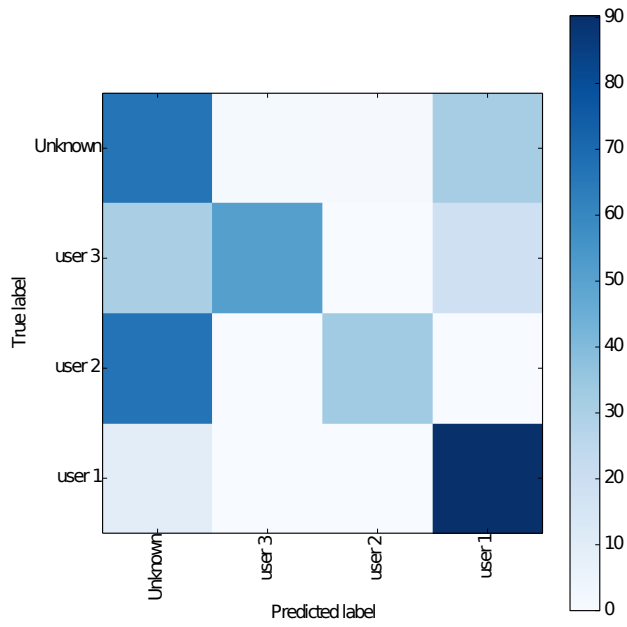


Figure 5.9: H3UV confusion matrix

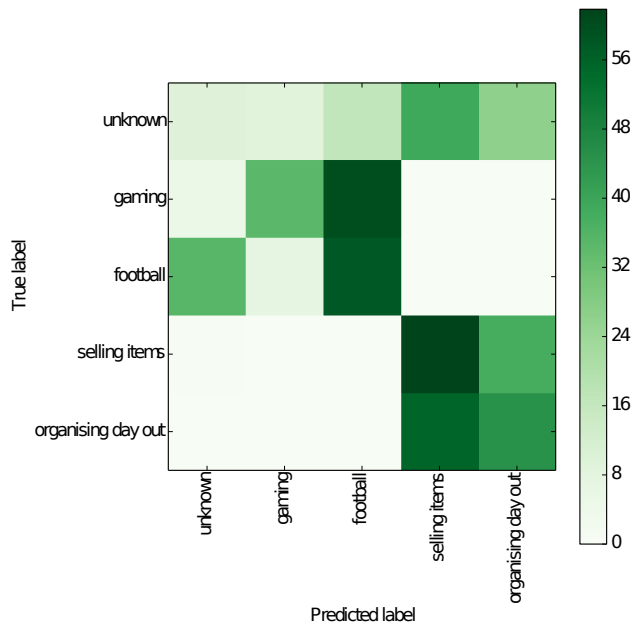


Figure 5.10: H3AV confusion matrix

---

	precision	recall	f1-measure	support
Unknown	0.76	0.53	0.62	48711
user 1	0.46 (0.82)	0.54	0.49 (0.65)	12254
user 2	0.35 (0.95)	0.67	0.46 (0.78)	13928
avg / total	0.63 (0.89)	0.56	0.57 (0.68)	74893

Table 5.8: H4UV classification results, optimistic precision shown in ()

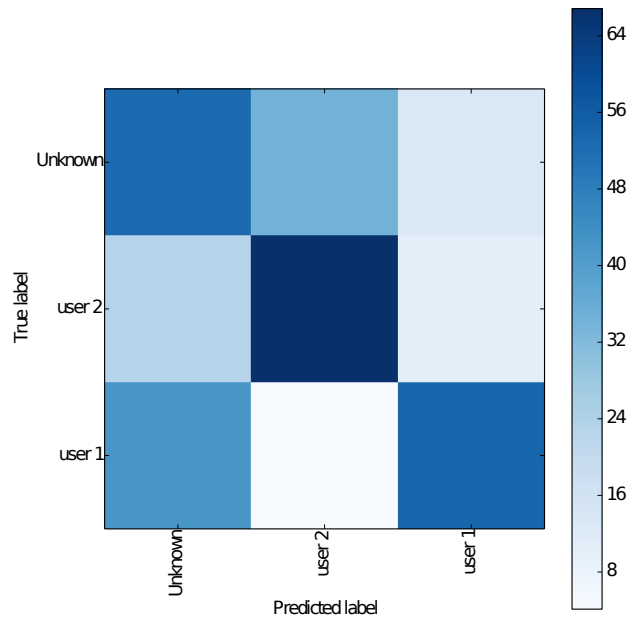


Figure 5.11: H4UV confusion matrix

**Activity classification** in Household 4 was omitted as there were no classes with sufficient support, available in both the training and validation datasets.

---

## 5.5 Discussion

The dataset used in this chapter is challenging to analyse with enterprise traffic classification techniques. The first challenge is the incomplete labelling of the data. A large proportion of data assigned to the Unknown class, which may contain real user generated traffic. This makes reporting the accuracy of the techniques difficult. However, it can be seen from the confusion matrices that in Household 3 reasonably good classification was achieved with a mean F1-measure of between 0.70 and 0.82.

This work considers each flow in isolation and attempts to assign it to a class, imitating the enterprise traffic classification techniques. This may not be the best tactic for users and activity classification in domestic environments. The IP Flows present within domestic environments cannot all be uniquely attributed to a user or/and activity. Some IP Flows will look identical, if requested on the same device, even if they are requested by different people. For example, DNS requests for the same domain or background images in websites. Only a small proportion of the IP Flows may be uniquely attributable to a particular user or activity. This is likely to be a contributing factor to the generally low recall observed across all households.

Another issue highlighted by this analysis is that the dynamic nature of the domestic environment can cause problems with classification performance. For example, adding a new device or a child returning from University. This type of change would need a different approach with the classifier being updated regularly. An online machine learning based strategy would be an appropriate technique to explore [11].

Classification performance for activities was poor in all households. Significant misclassification can be seen between classes in all confusion matrices. In only one or two instances were the classes reliably identified. The activity classification for Household 1 shows an interesting aspect of the activity classification. Some activities, that are strongly related or occur concurrently, can confuse the classifier. The likely cause of this is the mislabelling of IP flows due to the annotation to class label conversion step when assigning user annotations to flows.



---

In both the user classification and activity classification tasks the device MAC address was the most important feature. This suggests that there is a strong relationship between users, devices and, activities (see Figures 5.1 and 5.2). The amount of device sharing in a household will affect the classification performance.

Overall the direct application of enterprise traffic classification techniques to the HomeNetViewer dataset was disappointing. However, it shows some promise and opens up interesting questions for further research. To truly test the performance of a supervised learning approach, on this type of data, a new annotation method would need to be developed, that enabled IP flows to be annotated more accurately. The approach taken to assign labels to flows in this work has two problems. Firstly, it assumes all flows occurring on a device when a user is actively using it belong to them. This may not be the case, due to automated activities such as software updates and polling applications. Second, a large number of flows are unlabelled or incorrectly labelled. This makes assessing the classification performance difficult. How one could build a better annotation method, without over burdening the user, would be an interesting challenge to explore.

An area where this work could be improved would be to look at better feature engineering. The features used here were the minimum available. There are many more per-flow features that could be explored, with a more complete dataset. A second approach would be to explore calculating new features for groups of flows and using them as the input to the classification algorithms.

Furthermore, the techniques used in enterprise traffic classification are not the only machine learning techniques that may be useful in this domain. Machine learning is a large discipline, with many tools and techniques for dealing with different problems. There is the possibility of exploring semi-supervised approaches to deal with the misclassified Unknown data. Another approach would be to explore the use of an online stream learning algorithm [11]. This is where the learning algorithm is able to interactively query the user for further information to assist in the classification process.

# Chapter 6

## Conclusion

### 6.1 Key lessons

#### 6.1.1 User-centred mechanisms for domestic network infrastructure control

MultiNet was designed to address the problems with Wi-Fi device association in domestic environments. The user-centred design process applied was successful in achieving this objective. The process undertaken allowed the benefits of Out-of-Band communication channels to be implemented in a way that integrates into the domestic context. The lab based usability evaluation of MultiNet has shown it to be more usable than the currently deployed usable association method, WPS.

Three wider lessons that can be drawn from the exploration of user-centred mechanisms for domestic network infrastructure control. These address the overarching question: how should domestic networks be reinvented to support self-management by domestic users?

Firstly, reinventing the device association process for domestic environments did not require re-engineering the underlying protocols. Relatively small changes in the high-level implementations enabled the creation of a vastly different user interaction and Wi-Fi device association mechanism. The complex underlying communication and security protocols were untouched, significantly reducing the

---

complexity of the modifications. This shows that reinventing the domestic network infrastructure may not always be a significant engineering task.

Second, exploiting the home context is beneficial. For example, in the case of MultiNet, the physical security of the home was leveraged to provide a threat model that domestic users could understand, and a simple consistent user interaction. The domestic environment has many rituals and routines that may be worth exploring to address other issues.

Finally, providing an interface as a single point of management for domestic networks is beneficial. Our participants found using a mobile device to interact with the network infrastructure simple and intuitive. This supports the findings of other work [20, 95], but expanded it beyond situated displays onto mobile devices. Additionally, the Network Controller may enable a number of other domestic networking issues to be solved, by using the new interaction capabilities offered by this new piece of infrastructure.

### **6.1.2 User-centred presentations of network activity**

The deployment of HomeNetViewer was successful in its primary goal, increasing domestic network legibility. Applying a user-centred design process enabled the creation of a usable interactive network data visualisation and annotation platform. The user-centred design process provided focus, when building the prototype interfaces. This focus on the annotation process helped narrow down the relevant data to show to the users in the interfaces. The task of annotating network data was achieved by all participants with little or no training. This shows that interactive time-line visualisations are appropriate for visualising domestic network data. Also, all participants made comments that showed that HomeNetViewer increased their knowledge of the activities occurring on their networks.

The most informative data available to the domestic access point for use in the annotation process were the search term data. Search term data are, however, difficult to obtain and raised privacy concerns. The host and domain names extracted from the HTTP headers and DNS request were also informative and

---

useful in the annotation process, with the DNS request being the easiest and most reliably captured.

Participants were comfortable using hosts and domains to annotate data. They could identify hosts and domains they were familiar with and assign the appropriate activities in most cases. Some hosts and domains were also found to have strong relationships with certain users. These relationships were obvious to other members of the household. This tallies with the finding of Brundel et al., who found users reason about their network usage in terms of activities, application, and users [18].

Overall the deployment of HomeNetViewer shows that user-centred presentations of network activity improve network legibility. However, HomeNetViewer is not perfect, and several open challenges that are discussed in Section 6.2.

### **6.1.3 Automatic generation of User-centred presentations from IP Flow records**

The work undertaken on improving domestic network legibility through user-centred presentations of network activity, found that the manual annotation process was time consuming. All of the participants commented that the annotation process took too long.

A number of factors that negatively impact on annotation time are discussed in Section 4.4. Chapter 5 looked at addressing the annotation burden, by applying enterprise traffic classification techniques to domestic traffic in an attempt to answer the question: can enterprise traffic classification techniques be used with user contributed annotations to automatically annotate domestic network traffic?

Initial data analysis shows that the tree based classifiers perform best on the HomeNetViewer dataset, with the Random Forest classifier performing best in both user and activity classification tasks. This is in keeping with the findings of Grimaudo [36].

This work shows that automatic generation user annotations by directly applying enterprise traffic classification techniques is challenging. While the classifier was better than random guessing, there was significant confusion between users in all households. For the automatic generation of activity annotations the results

---

were less encouraging. Even after the activities with good support in both the training and validation sets were chosen, the classifier still struggled to accurately classify traffic into activities.

However, it is worth noting that this was a particularly challenging dataset. It was manually annotated by unskilled users, and was not specifically collected to support a machine learning based approach. Large sections of the dataset were not annotated and the coverage of actual user activity is not complete. This, combined with inaccuracy introduced by transferring time-based annotations to the IP Flow data, made the classification task more difficult, reducing the overall reported F1-measures.

## **6.2 Open challenges**

### **6.2.1 User-centred mechanisms for domestic network infrastructure control**

The introduction of the network controller by MultiNet was well received by the participants. The network controller, in this case, was a mobile phone that offers rich interaction capabilities. The extra interaction capabilities opens new possibilities in designing interactions with the domestic network infrastructure. Exploring these further could prove fruitful.

### **6.2.2 User-centred presentations of network activity**

This work has left several open changes, and directions for future research. Firstly, how to reduce the annotation time for users is an open question. Would better interfaces or an automated traffic classification approach be the better solution? Or possibly a combination of the two? User-centred presentations of network activity have clear benefits, but unless a more efficient annotation method can be found wider adoption is unlikely.

The second challenge is how to leverage the information within search term data without exposing sensitive information? The search term data were a valuable source of information. Some users relied on it to perform the annotation

---

task. However, most of the participants in the deployment were unhappy at the level of information that it exposed, even to close family members. Removing the search term data from the interfaces would make annotation even more time consuming, further burdening the users.

The third, challenge is the identification and removal of automated traffic and device/application specific behaviours. The automated traffic and device/application specific behaviours cluttered the interfaces and reduced the effectiveness of HomeNetViewer in two ways. One, it clutters the visualisations obscuring true user activity. Two, it clutters the annotation interfaces, increasing the time taken to process the list of visited hosts. Fully addressing this challenge would improve the user experience and also the quality of the resulting annotations.

Finally, the one-to-one mapping between users and activities and domains is insufficient in some cases. Not only do some host/domains have multiple activities, but the reason for visiting the host/domain could be user dependent. Improvements to the annotation interface to take into account websites with multiple activities and users with differing activities would be a challenging issue to address.

### **6.2.3 Automatic generation of User-centred presentations from IP Flow records**

This work has outlined three open challenges. Firstly, exploring improved machine learning techniques for processing human annotated network datasets. The machine learning techniques, used in enterprise traffic classification, were built around fully annotated datasets. They do not need to cope with missing data and/or evolving behaviours. Classifying domestic traffic using user generated annotations is different. The presence of unknown data, mislabelled data and rapidly changing behaviour patterns due the ebb and flow of daily life. Creating a system to deal with these factors is a significant challenge.

Second, the development of more accurate IP flow annotation platforms for domestic environments. Improving the machine learning techniques applied is one way forward. Another possible avenue to explore would be to improve the

---

annotation interfaces, specifically focusing on improving the accuracy of IP flow annotations.

Finally, one important question that remains is how accurate do the automatic classification of network traffic need to be to support the self-management by users? To provide useful information to domestic users 100% accuracy may not be required. Interfaces that express the confidence that a particular activity was performed by a particular user could be good enough to support local negotiation of domestic network policy.

### 6.3 Next steps

MultiNet and HomeNetViewer demonstrate that reinventing the domestic network infrastructure taking a user-centred design approach has a positive impact on domestic Wi-Fi device association and network legibility. The two case studies show that the application of user-centred design approach to domestic network redesign produces usable solutions to these specific problems. However, this dissertation only addressed two particular issues with domestic networks. Further work is required to explore user-centred solutions for other aspects of domestic network management and configuration.

This dissertation leaves several interesting future challenges regarding the processing of data passing through domestic access points. The main complaint made by participants regarding the use of HomeNetViewer was the time taken to perform the annotation task. The application of enterprise traffic classification techniques shows some promise.

However, the techniques currently used do not handle the HomeNetViewer dataset well. This leaves two angles to explore in future work. Firstly, building interfaces specifically designed to annotate IP flow data more accurately. Second, the exploration of better machine learning techniques that are designed to cope with this type of dataset. One possibility would be to use an online stream learning approach [11]. This has the benefit of engaging the user in the classification process and constantly updates its model for each new sample received.

The second challenge is how to use the data passing through domestic access points in a way the domestic users are comfortable with. The amount of informa-

---

tion exposed to other householders was problematic. Once again the application of machine learning techniques may also help address these privacy issues. This would require the collection of many annotated datasets to enable development of algorithms to identify activities that are universally identifiable between households. Automation of the annotation process would reduce, or remove altogether, the need to expose the underlying data for annotation by the user.

As households embrace new trends towards IoT enabled devices, the physical complexity and amount of data passing through domestic network is only set to increase. The domestic access point provides an important means of configuration, visibility and control over this developing infrastructure. This dissertation demonstrates that reinventing the domestic network to support self-management by domestic users can resolve the existing problems with domestic networking infrastructure and merits further research, exploration by industry and standardisation bodies.



# References

- [1] IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements. *IEEE Std 802.11i-2004* (July 2004), 1–190. 11
- [2] IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications. *IEEE Std 1901-2010* (Dec 2010), 1–1586. 10
- [3] IEEE Standard for Ethernet - Section 1. *IEEE Std 802.3-2012 (Revision to IEEE Std 802.3-2008)* (Dec 2012), 1–0. 10
- [4] IEEE Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)* (March 2012), 1–2793. 10, 22, 57
- [5] ALLIANCE, W.-F. Wi-fi protected setup specification. *WiFi Alliance Document* (2007). 23
- [6] AMIN, R., JACKSON, F., GILBERT, J. E., MARTIN, J., AND SHAW, T. Assessing the impact of latency and jitter on the perceived quality of call of duty modern warfare 2. In *Human-Computer Interaction. Users and Contexts of Use*. Springer, 2013, pp. 97–106. 54

## REFERENCES

---

- [7] BALFANZ, D., DURFEE, G., AND GRINTER, R. E. Network-in-a-box: how to set up a secure wireless network in under a minute. In *Proc. 13th USENIX Security Symposium* (2004), USENIX Association. 25
- [8] BALFANZ, D., SMETTERS, D. K., AND STEWART, P. Talking to strangers: Authentication in ad-hoc wireless networks. In *Proc. NDSS* (2002). 24
- [9] BANGOR, A., KORTUM, P. T., AND MILLER, J. T. An Empirical Evaluation of the System Usability Scale. *International Journal of Human-Computer Interaction* 24, 6 (July 2008), 574–594. 50
- [10] BATES, O., AND BROADBENT, M. HomeFlow: Inferring Device Usage with Network Traces. In *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication* (New York, NY, USA, 2013), UbiComp '13 Adjunct, ACM, pp. 815–820. 26
- [11] BIFET, A. Adaptive stream mining: Pattern learning and mining from evolving data streams. In *Proceedings of the 2010 conference on adaptive stream mining: Pattern learning and mining from evolving data streams* (2010), Ios Press, pp. 1–212. 123, 124, 130
- [12] BISHOP, C. *Pattern Recognition and Machine Learning*. Information Science and Statistics. Springer, 2006. 103
- [13] BLY, S., SCHILIT, B., McDONALD, D. W., ROSARIO, B., AND SAINT-HILAIRE, Y. Broken expectations in the digital home. In *CHI '06 extended abstracts on Human factors in computing systems* (2006), CHI EA '06, ACM, pp. 568–573. 2, 9
- [14] BOUZAKARIA, N., CONCOLATO, C., AND LE FEUVRE, J. Overhead and performance of low latency live streaming using mpeg-dash. In *Information, Intelligence, Systems and Applications, IISA 2014, The 5th International Conference on* (2014), IEEE, pp. 92–97. 55
- [15] BROOKE, J. SUS— a quick and dirty usability scale. *Usability evaluation in industry 189* (1996), 194. 49

- 
- [16] BROWN, A., MORTIER, R., AND RODDEN, T. Multinet: Reducing interaction overhead in domestic wireless networks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2013), CHI '13, ACM, pp. 1569–1578. iv, 6, 39
- [17] BROWN, A., MORTIER, R., AND RODDEN, T. An exploration of user recognition on domestic networks using netflow records. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication* (2014), UbiComp '14 Adjunct, ACM, pp. 903–910. 7
- [18] BRUNDELL, P., CRABTREE, A., MORTIER, R., RODDEN, T., TENNENT, P., AND TOLMIE, P. The network from above and below. In *Proceedings of the first ACM SIGCOMM workshop on Measurements up the stack* (New York, NY, USA, 2011), W-MUST '11, ACM, pp. 1–6. 14, 25, 28, 62, 94, 102, 127
- [19] CERF, V., AND KAHN, R. A protocol for packet network intercommunication. *Communications, IEEE Transactions on* 22, 5 (May 1974), 637–648. 11
- [20] CHETTY, M., BANKS, R., HARPER, R., REGAN, T., SELLEN, A., GKANTSIDIS, C., KARAGIANNIS, T., AND KEY, P. Who's hogging the bandwidth: the consequences of revealing the invisible in the home. In *Proceedings of the 28th international conference on Human factors in computing systems* (2010), pp. 659–668. 3, 26, 98, 126
- [21] CLAISE, B., AND TRAMMELL, B. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information. RFC 7011, ietf, sept 2013. 66, 105
- [22] COSTANZA, E., RAMCHURN, S. D., AND JENNINGS, N. R. Understanding domestic energy consumption through interactive visualisation: a field study. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (2012), pp. 216–225. 26, 63, 69

## REFERENCES

---

- [23] COTTON, M., EGGERT, L., TOUCH, J., WESTERLUND, M., AND CHESHIRE, S. Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry. RFC 6335, IETF, Aug. 2011. 27
- [24] CRABTREE, A., MORTIER, R., RODDEN, T., AND TOLMIE, P. Unremarkable networking: the home network as a part of everyday life. In *Proceedings of the Designing Interactive Systems Conference* (New York, NY, USA, 2012), DIS '12, ACM, pp. 554–563. 2, 9, 22
- [25] CRABTREE, A., AND RODDEN, T. Domestic routines and design for the home. *Computer Supported Cooperative Work (CSCW)* 13, 2 (2004), 191–220. 13
- [26] CRABTREE, A., RODDEN, T., TOLMIE, P., MORTIER, R., LODGE, T., BRUNDELL, P., AND PANTIDI, N. House rules: the collaborative nature of policy in domestic networks. *Personal and Ubiquitous Computing* (2014), 1–13. 15, 16, 19, 62
- [27] DOURISH, P., GRINTER, E., DELGADO DE LA FLOR, J., AND JOSEPH, M. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal Ubiquitous Comput.* 8, 6 (Nov. 2004), 391–401. 18
- [28] DROMS, R. Dynamic Host Configuration Protocol. RFC 2131, IETF, Mar. 1997. 11
- [29] EDWARDS, W., AND GRINTER, R. At home with ubiquitous computing: Seven challenges. In *UbiComp 2001: Ubiquitous Computing*, vol. 2201 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2001, pp. 256–272. 2, 9
- [30] EDWARDS, W. K., GRINTER, R. E., MAHAJAN, R., AND WETHERALL, D. Advancing the state of home networking. *Commun. ACM* 54, 6 (June 2011), 62–71. 13

- 
- [31] EDWARDS, W. K., NEWMAN, M. W., AND POOLE, E. S. The infrastructure problem in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010), ACM, pp. 423–432. 2, 18, 20
- [32] FEAMSTER, N. Outsourcing home network security. In *Proceedings of the 2010 ACM SIGCOMM Workshop on Home Networks* (New York, NY, USA, 2010), HomeNets '10, ACM, pp. 37–42. 18
- [33] FOROUZAN, B. A. *TCP/IP Protocol Suite*, 2 ed. McGraw-Hill, Inc., New York, NY, USA, 2002. 10
- [34] GOODRICH, M., SIRIVIANOS, M., SOLIS, J., TSUDIK, G., AND UZUN, E. Loud and clear: Human-verifiable authentication based on audio. In *Proc. IEEE 26th ICDCS* (2006), p. 10. 25
- [35] GOULD, J. D., AND LEWIS, C. Designing for usability: Key principles and what designers think. *Commun. ACM* 28, 3 (Mar. 1985), 300–311. 3
- [36] GRIMAUDO, L., MELLIA, M., BARALIS, E., AND KERALAPURA, R. Self-learning classifier for internet traffic. In *INFOCOM, 2013 Proceedings IEEE* (April 2013), pp. 3381–3386. 107, 108, 127
- [37] GRINTER, R. E., EDWARDS, W. K., CHETTY, M., POOLE, E. S., SUNG, J.-Y., YANG, J., CRABTREE, A., TOLMIE, P., RODDEN, T., GREENHALGH, C., AND BENFORD, S. The ins and outs of home networking: The case for useful and usable domestic networking. *ACM Trans. Comput.-Hum. Interact.* 16, 2 (June 2009), 8:1–8:28. 17
- [38] GRINTER, R. E., EDWARDS, W. K., NEWMAN, M. W., AND DUCHENEAUT, N. The work to make a home network work. In *ECSCW 2005*. Springer Netherlands, 2005, pp. 469–488. 13, 15, 17, 19
- [39] HEMEL, A. Universal plug and play: Dead simple or simply deadly? In *5th System Administration and Network Engineering Conference, Delft, The Netherlands* (2006). 19
- [40] HENDERSON, T. N. H. *The effects of relative delay in networked games*. PhD thesis, Citeseer, 2003. 54

## REFERENCES

---

- [41] HERRMANN, D., BANSE, C., AND FEDERRATH, H. Behavior-based tracking: Exploiting characteristic patterns in DNS traffic. *Computers & Security* 39, Part A (Nov. 2013), 17–33. 29
- [42] HO, J. T., AND DEARMAN, D. Improving users’ security choices on home wireless networks. In *Proc. 6th SOUPS* (2010), ACM, pp. 1–12. 17, 18, 21, 23
- [43] HUTCHINSON, H., MACKAY, W., WESTERLUND, B., BEDERSON, B. B., DRUIN, A., PLAISANT, C., BEAUDOUIN-LAFON, M., CONVERSY, S., EVANS, H., HANSEN, H., ROUSSEL, N., AND EIDERBCK, B. Technology probes: Inspiring design for and with families. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2003), CHI '03, ACM, pp. 17–24. 4
- [44] KARAGIANNIS, T., PAPAGIANNAKI, K., AND FALOUTSOS, M. BLINC: multilevel traffic classification in the dark. In *ACM SIGCOMM Computer Communication Review* (2005), vol. 35, ACM, pp. 229–240. 28
- [45] KIESLER, S., ZDANIUK, B., LUNDMARK, V., AND KRAUT, R. Troubles with the internet: The dynamics of help at home. *Human-Computer Interaction* 15, 4 (2000), 323–351. 17
- [46] KLASNJA, P., CONSOLVO, S., JUNG, J., GREENSTEIN, B. M., LEGRAND, L., AND POWLEDGE. “when i am on wi-fi, i am fearless”: privacy concerns & practices in everyday wi-fi use. In *Proc. 27th ACM CHI* (2009), ACM. 44
- [47] KOBZA, A., SONAWALLA, R., TSUDIK, G., UZUN, E., AND WANG, Y. Serial hook-ups: a comparative usability study of secure device pairing methods. In *Proc. 5th SOUPS* (2009), ACM, pp. 1–12. 25
- [48] KOHAVI, R. A study of cross-validation and bootstrap for accuracy estimation and model selection. In *Proceedings of the 14th International Joint Conference on Artificial Intelligence - Volume 2* (San Francisco, CA, USA, 1995), IJCAI'95, Morgan Kaufmann Publishers Inc., pp. 1137–1143. 108

## REFERENCES

---

- [49] KUMAR, A., SAXENA, N., TSUDIK, G., AND UZUN, E. Caveat emptor: A comparative study of secure device pairing methods. In *Proc. IEEE PerCom* (Mar. 2009), pp. 1–10. 25
- [50] KUMPO\VST, M., AND MATY\VS, V. User profiling and re-identification: Case of university-wide network analysis. In *Trust, Privacy and Security in Digital Business*. Springer, 2009, pp. 1–10. 30
- [51] KUO, C., WALKER, J., AND PERRIG, A. Low-cost manufacturing, usability, and security: An analysis of Bluetooth simple pairing and Wi-Fi protected setup. In *Proc. FC'07/USEC'07* (2007), Springer-Verlag. 44
- [52] KUO, C., WALKER, J., AND PERRIG, A. Low-cost manufacturing, usability, and security: An analysis of bluetooth simple pairing and wi-fi protected setup. In *Financial Cryptography and Data Security*, S. Dietrich and R. Dhamija, Eds., vol. 4886 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2007, pp. 325–340. 44
- [53] LIM, Y., PARK, K., LEE, J. Y., AOKI, S., AND FERNANDO, G. Mmt: An emerging mpeg standard for multimedia delivery over the internet. *MultiMedia, IEEE* 20, 1 (2013), 80–85. 55
- [54] MAYRHOFER, R., AND GELLERSEN, H. Shake well before use: Authentication based on accelerometer data. In *Pervasive Computing*, A. LaMarca, M. Langheinrich, and K. N. Truong, Eds., no. 4480 in *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, Jan. 2007, pp. 144–161. 25
- [55] MCCUNE, J., PERRIG, A., AND REITER, M. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *Proc. IEEE Symposium on Security and Privacy* (May 2005), pp. 110–124. 24
- [56] MELNIKOV, A., LEIBA, B., AND LI, K. Universal Plug and Play (UPnP) Internet Gateway Device - Port Control Protocol Interworking Functio. RFC 6970, IETF, July 2013. 19
- [57] MERKLE, R. C. Secure communications over insecure channels. *Commun. ACM* 21, 4 (Apr. 1978), 294–299. 23

## REFERENCES

---

- [58] MOALLEM, A. Home networking: Smart but complicated. In *Human-Computer Interaction. Applications and Services*, M. Kurosu, Ed., no. 8512 in Lecture Notes in Computer Science. Springer International Publishing, Jan. 2014, pp. 731–741. 12, 13
- [59] MOCKAPETRIS, P. Domain names – implementation and specification. RFC 1035, IETF, Nov. 1987. 11
- [60] MOORE, A., ZUEV, D., AND CROGAN, M. *Discriminators for use in flow-based classification*. Queen Mary and Westfield College, Department of Computer Science, 2005. 105
- [61] MOORE, A. W., AND PAPAGIANNAKI, K. Toward the accurate identification of network applications. In *Proceedings of the 6th International Conference on Passive and Active Network Measurement* (Berlin, Heidelberg, 2005), PAM’05, Springer-Verlag, pp. 41–54. 27
- [62] MOORE, A. W., AND ZUEV, D. Internet traffic classification using bayesian analysis techniques. In *Proceedings of the 2005 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems* (New York, NY, USA, 2005), SIGMETRICS ’05, ACM, pp. 50–60. 28
- [63] MORTIER, R., RODDEN, T., TOLMIE, P., LODGE, T., SPENCER, R., SVENTEK, J., AND KOLIOUSIS, A. Homework: putting interaction into the infrastructure. In *Proceedings of the 25th annual ACM symposium on User interface software and technology* (2012). 3, 20, 64, 65
- [64] NORMAN, D. A., AND DRAPER, S. W. User centered system design. *New Perspectives on Human-Computer Interaction*, L. Erlbaum Associates Inc., Hillsdale, NJ (1986). 3
- [65] O’BRIEN, J., AND RODDEN, T. Interactive systems in domestic environments. In *Proceedings of the 2nd conference on Designing interactive systems: processes, practices, methods, and techniques* (New York, NY, USA, 1997), DIS ’97, ACM, pp. 247–259. 14



## REFERENCES

---

- [66] PEDREGOSA, F., VAROQUAUX, G., GRAMFORT, A., MICHEL, V., THIRION, B., GRISEL, O., BLONDEL, M., PRETTENHOFER, P., WEISS, R., DUBOURG, V., VANDERPLAS, J., PASSOS, A., COURNAPEAU, D., BRUCHER, M., PERROT, M., AND DUCHESNAY, E. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research* 12 (2011), 2825–2830. 107
- [67] POOLE, E., EDWARDS, W., AND JARVIS, L. The home network as a socio-technical system: Understanding the challenges of remote home network problem diagnosis. *Computer Supported Cooperative Work (CSCW)* 18, 2-3 (2009), 277–299. 17
- [68] POOLE, E. S., CHETTY, M., GRINTER, R. E., AND EDWARDS, W. K. More than meets the eye: transforming the user experience of home network management. DIS '08, ACM, pp. 455–464. 13, 14, 41
- [69] POOLE, E. S., CHETTY, M., MORGAN, T., GRINTER, R. E., AND EDWARDS, W. K. Computer help at home: Methods and motivations for informal technical support. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2009), CHI '09, ACM, pp. 739–748. 17
- [70] POSTEL, J. User Datagram Protocol. RFC 768, IETF, Aug. 1980. 11
- [71] POSTEL, J. Internet Protocol. RFC 791, IETF, Sept. 1981. 11
- [72] POSTEL, J. Transmission Control Protocol. RFC 793, IETF, Sept. 1981. 11
- [73] PREECE, J., SHARP, H., AND ROGERS, Y. *Interaction Design-beyond human-computer interaction*. John Wiley & Sons, 2015. 3
- [74] ROLLINS, S., BANERJEE, N., CHOUDHURY, L., AND LACHUT, D. A system for collecting activity annotations for home energy management. *Pervasive and Mobile Computing* 15 (2014), 153 – 165. Special Issue on Information Management in Mobile ApplicationsSpecial Issue on Data Mining in Pervasive Environments. 26

## REFERENCES

---

- [75] SASSE, M. A., BROSTOFF, S., AND WEIRICH, D. Transforming the ‘weakest link’ – a human/computer interaction approach to usable and effective security. *BT Technology Journal* 19 (2001), 122–131. 23
- [76] SAWERS, P. UK Homes Have 5 WiFi Devices Connected, Dec. 2011. 59
- [77] SAXENA, N., EKBERG, J.-E., AND KOSTIAINEN, K. Secure Device Pairing Based on a Visual Channel: Design and Usability Study. *IEEE Trans. Information Forensics and Security* 6, 1 (2011), 28–38. 24
- [78] SCHULZRINNE, H., RAO, A., AND LANPHIER, R. Real Time Streaming Protocol (RTSP). RFC 2326, IETF, Apr. 1998. 54
- [79] SHEHAN, E., AND EDWARDS, W. K. Home networking and HCI: what hath god wrought? In *Proceedings of the SIGCHI conference on Human factors in computing systems* (2007), pp. 547–556. 2, 9, 16
- [80] SHEHAN, E., AND EDWARDS, W. K. Home networking and HCI: What hath God wrought? In *Proc. ACM CHI* (2007), ACM, pp. 547–556. 44
- [81] SORIENTE, C., TSUDIK, G., AND UZUN, E. Hapadep: Human-assisted pure audio device pairing. In *Information Security*, vol. 5222 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2008. 25
- [82] STAJANO, F., AND ANDERSON, R. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Security Protocols*, vol. 1796 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2000. 24
- [83] STEINBERG, D. H., AND CHESHIRE, S. *Zero Configuration Networking: The Definitive Guide: The Definitive Guide.* ” O’Reilly Media, Inc.”, 2005. 19
- [84] SUNDARESAN, S., DE DONATO, W., FEAMSTER, N., TEIXEIRA, R., CRAWFORD, S., AND PESCAPÈ, A. Broadband internet performance: a view from the gateway. *ACM SIGCOMM computer communication review* 41, 4 (2011), 134–145. 54

## REFERENCES

---

- [85] SUNDARESAN, S., FEAMSTER, N., TEIXEIRA, R., GRUNENBERGER, Y., PAPAGIANNAKI, D., AND LEVIN, D. Characterizing Home Network Performance Problems. Tech. rep., Sept. 2013. 17
- [86] SVENTEK, J., KOLIOUSIS, A., SHARMA, O., DULAY, N., PEDIADITAKIS, D., SLOMAN, M., RODDEN, T., LODGE, T., BEDWELL, B., GLOVER, K., AND MORTIER, R. An information plane architecture supporting home network management. In *2011 IFIP/IEEE International Symposium on Integrated Network Management (IM)* (2011), pp. 1–8. 20
- [87] TASOLUK, B., AND TANRIKULU, Z. A weakest chain approach to assessing the overall effectiveness of the 802.11 wireless network security. *CoRR abs/1103.0464* (2011). 44
- [88] TOLMIE, P., CRABTREE, A., RODDEN, T., GREENHALGH, C., AND BENFORD, S. Making the home network at home: Digital housekeeping. In *ECSCW 2007*. Springer London, 2007, pp. 331–350. 15, 19
- [89] TOLMIE, P., CRABTREE, A., RODDEN, T., GREENHALGH, C., AND BENFORD, S. Making the home network at home: Digital housekeeping ECSCW, springer/kluwer. In *In Proceedings of the European Conference on Computer-Supported Cooperative Work* (2007). 19
- [90] TORAL, H., TORRES, D., HERNÁNDEZ, C., AND ESTRADA, L. Self-similarity, packet loss, jitter, and packet size: empirical relationships for voip. In *Electronics, Communications and Computers, 2008. CONIELECOMP 2008, 18th International Conference on* (2008), IEEE, pp. 11–16. 54
- [91] VIEHBÖCK, S. Us-cert vulnerability note vu#723755 - wifi protected setup (wps) pin brute force vulnerability, 2011. 24
- [92] WANG, X. S., BALASUBRAMANIAN, A., KRISHNAMURTHY, A., AND WETHERALL, D. Demystifying page load performance with wprof. In *Presented as part of the 10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13)* (2013), pp. 473–485. 54

## REFERENCES

---

- [93] WASH, R. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (New York, NY, USA, 2010), SOUPS '10, ACM, pp. 11:1–11:16. 18
- [94] WI-FI ALLIANCE. Wi-Fi Protected Setup. <http://www.wi-fi.org/discover-wi-fi/wi-fi-protected-setup>, 2010. 46
- [95] YANG, J., AND EDWARDS, W. Icebox: Toward easy-to-use home networking. In *Human-Computer Interaction INTERACT 2007*, vol. 4663 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2007, pp. 197–210. 19, 26, 126
- [96] YANG, J., EDWARDS, W. K., AND HASLEM, D. Eden: supporting home network management through interactive visual tools. In *Proceedings of the 23rd annual ACM symposium on User interface software and technology* (New York, NY, USA, 2010), UIST '10, ACM, pp. 109–118. 26
- [97] YANG, Y. C. Web user behavioral profiling for user identification. *Decision Support Systems* 49, 3 (June 2010), 261–271. 30