



Received: 23 January 2018  
Accepted: 18 April 2018  
First Published: 18 May 2018

\*Corresponding author: Ahmed Al-Haiqi, Department of Electronics and Communication Engineering, Universiti Tenaga Nasional, SQ6-6-1 Staff Quarters, UNITEN, Jalan Ikram-Uniten, Kajang, Malaysia.  
E-mail: [ahmedmubarak@uniten.edu.my](mailto:ahmedmubarak@uniten.edu.my)

Reviewing editor:  
Chau Yuen, Singapore University of Technology and Design, Singapore

Additional information is available at the end of the article

## COMPUTER SCIENCE | REVIEW ARTICLE

# SDN in the home: A survey of home network solutions using Software Defined Networking

Abdalkrim M. Alshnta<sup>1</sup>, Mohd Faizal Abdollah<sup>1</sup> and Ahmed Al-Haiqi<sup>2\*</sup>

**Abstract:** Software Defined Networking (SDN) is an important paradigm shift of computer networking in the last 10 years. The concept of SDN is so powerful that the potential of applying it can easily be perceived beyond the initial use case of large data centre networks. We are motivated by this perception to explore the potential use of SDN in the context of home networks specifically, even though home environments were not the driving scenario behind SDN in the first years of its development. Lacking other reviews on the subject, we performed a focused search for every article that proposes, discusses or otherwise addresses the idea of implementing SDN in home networking. We surveyed four major technical and online databases (IEEE Xplore, ACM, ScienceDirect and Wiley) to ensure the inclusion of relevant, quality and authentic works. The final filtered set included 42 articles that spanned the period from 2010 to 2017. Most of the articles address specific aspects of controlling and managing home networks, such as Quality of Experience, security, Internet caps, Internet-of-Things device management and other specific themes, while the rest of articles address the generic case of managing home networks using SDN without a special focus on a particular target application. We derive a simple taxonomy for the works on home SDN and summarize the complete

### ABOUT THE AUTHOR

The work in this paper is part of a series of investigations on the emerging SDN technology and its applications in:

- Home network management
- Network security
- Smart home implications
- Privacy-aware smart metering in consumer households

Some of these topics are addressed in grant-based projects while others are part of our undergraduate students' projects. These projects are a joint collaboration between Universiti Teknikal Malaysia Melaka, Faculty of Information and Communication Technology (INSFORNET research group) and Universiti Tenaga Nasional, Department of Electronic and Communications Engineering.

### PUBLIC INTEREST STATEMENT

In the past, *home networks* used to be small, connecting a couple of computers to the Internet, mainly for browsing websites. Today, these networks are complex, connecting various devices, from computers and smartphones to TVs and Internet-of-Things (IoT) devices. Our applications have grown from simple web browsing to live video streaming. Our diverse needs require complicated configuration that cannot be managed by occasional calls to technical support. Unfortunately, current networking technology expects low-level knowledge that is beyond the average user, and specialists cannot simplify this task for non-specialists (a common practice in IT industry) because there is no *open interfaces*, and no *programmability*. These are the keywords that SDN is addressing. Though SDN is primarily driven by applications of data centres, researchers started to explore its application in home networks to give home users the control over their networks. The purpose of this article is to survey and summarize the landscape of research on this particular topic for the networking community and the general public.

set of works, highlighting few points along the way and drawing few simple statistics.

**Subjects: Management of IT; Systems and Computer Engineering; Networks; Communication Technology; Communication Networks and Systems**

**Keywords: home networks; software defined home networks; OpenFlow; SDN**

## 1. Introduction

Software Defined Networking (SDN) is the latest major trend in computer networking that promises to create a whole paradigm shift. The formulation of SDN started in academia in 2008 as a response to the difficulties that face professionals in managing today's networks. The problem of current network appliances is that they are typically manufactured by individual vendors and combine the essential functions of forwarding packets along with proprietary control software to control those functions. Proprietary interfaces are usually used to configure the devices for higher-level policies. As a result, the management of network functions is closely tied to the individual hardware devices, which in turn are associated with individual vendors and proprietary interfaces.

The whole idea behind SDN is to introduce a separation between the actual forwarding functions of the network that can be performed in hardware (collectively named as the forwarding layer of the network) and the management of those functions that can be expressed in software (collectively named as the control plane of the network). This separation of concerns holds the promise of more flexible network architecture that allows for innovation, and eases the task of network management.

Despite the revolutionary impact that SDN carries to the whole scene of networking today, it is safe to state that the premier driver behind SDN is the modern data centre, where the sheer number of servers, the required agility of reconfigurations and the traffic patterns make the new features of SDN very attractive and in great demand. Nevertheless, the SDN technology can bring important innovations to other domains as well, especially when the level of complexity increases to the extent where traditional networks can offer little help. One particular domain that started to receive an increasing attention by network researchers is the management of home networks.

Home networks are getting harder to manage as more devices are connected, and new applications are introduced, spanning the whole range from home entertainment, communication and social networking up to performing work from home. Started as simple connections of user computers to the Internet, home networks have considerably evolved during the last decades, and the number of devices they connect is exploding: from an initial situation with a few PCs, a set-top-box and a residential Home Gateway, then the emergence of many multimedia devices (media servers, tablets, smartphones, connected TVs, etc.), and up to the recent arrival of consumer IoT devices such as connected thermostats and weather stations. Integrating these different devices into home networks is challenging as there are two contradicting requirements to increase their acceptance ratio: ease of use versus tight control of information flows to enforce user privacy and user preferences (e.g. controlling who accesses the devices and where collected information is sent).

In that regard, an interesting characteristic of SDN applied to the connected home is to greatly facilitate the home network management by virtualising the home network infrastructure. Based on this premise, a number of research studies started to address this potential application of SDN and explore the ways in which SDN can help put the control of home networks into the hands of their users. Despite the fact that this line of research is already active since the few last years, we cannot find a dedicated reference for the various works and proposals up to this point, perhaps except a single review on wireless software defined networks, which includes a brief section on wireless home networks (Haque & Abu-Ghazaleh, 2016). Out of this need, we set up to survey the

available works on this subject, summarising the researchers' efforts in applying SDN to the home and mapping the literature into a unified taxonomy.

## 2. Background

This section provides the necessary background to understand the general problem of home networking and the very nature of SDN that makes this new paradigm a very attractive solution for that problem. This is a brief treatment, and the interested reader is referred to (Edwards, Grinter, Mahajan, & Wetherall, 2011; Feamster, Rexford, & Zegura, 2014; Grinter et al., 2009; Goransson, Black, & Culver, 2016; Kreutz et al., 2015; Nunes, Mendonca, Nguyen, Obraczka, & Turletti, 2014).

### 2.1. The problem of home network management

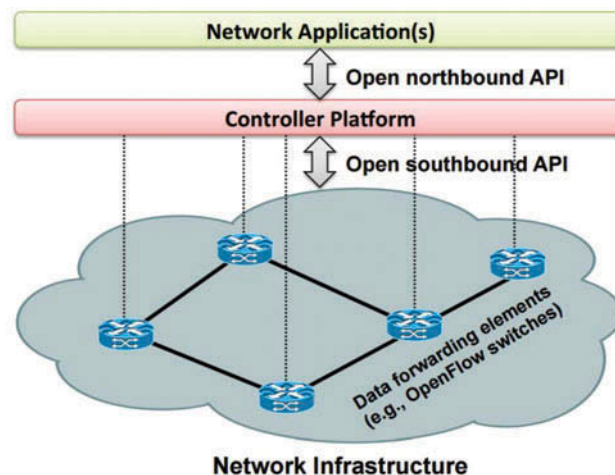
One major problem with managing home networks is the low-level configuration required to implement different controls, and the lack of this level of technical knowledge among home users. For example, a pertinent task in home networks is to manage the bandwidth of incoming broadband connection. If it is required to control the Internet usage cap, then there is a need to monitor the bandwidth usage and interfere when necessary. This functionality requires a level of statistical aggregation that is not easy to implement with current consumer switches and routers by home users. There is also no interface to report and then act upon those results. If the required control is bandwidth management with respect to individual devices or applications, then again, there is no easy way to implement this functionality with traditional networking devices in home. Similar functions can be found in larger networks (e.g. enterprise networks) using special middle boxes such as load balancers, but not in the home.

These types of control necessitate low-level configurations that are way beyond the capabilities of the average home user and that might require specialised network devices besides the typical home gateway. Obviously, a new model of configuring networking functions is needed, which can abstract the low-level details into higher-level control and provide a means of collecting an overall view of the network as well as an open interface to access network configuration. Here comes the role of SDN.

### 2.2. SDN architecture

The basic architecture of SDN is shown in Figure 1. The original design of SDN constitutes three major layers: infrastructure, controller and application layers as well as the interfaces between successive layers. From the bottom of the layered architecture in Figure 1, the infrastructure layer comprises network devices that perform packet forwarding, that is data forwarding; hence, the elements in this layer are also collectively called the data layer or the forwarding plane.

Figure 1. Basic architecture of SDN.



The first fundamental characteristic of SDN is the separation of the forwarding and control planes in network devices. The forwarding plane implements forwarding functionality, including the logic and tables for choosing how to deal with incoming packets, based on characteristics such as MAC address, IP address, and VLAN ID. The fundamental actions performed by the forwarding plane can be described by how it dispatches arriving packets. It may forward, drop, consume, or replicate an incoming packet. It may also transform the packet in some manner before taking further action. For basic forwarding, the device determines the correct output port by performing a lookup in the address table in the hardware switch or router. A packet may be dropped due to buffer overflow conditions or due to specific filtering resulting from a quality of service (QoS) rate-limiting function, for example.

The logic and algorithms that are used to program the forwarding plane reside in the control plane. Many of these protocols and algorithms require global knowledge of the network. The control plane determines how the forwarding tables and logic in the data plane should be programmed or configured. Since in a traditional network each device has its own control plane, the primary task of that control plane is to run routing or switching protocols so that all the distributed forwarding tables on the devices throughout the network stay synchronised. In SDN, the control plane is moved off of the switching device and onto a centralised controller.

Building on the idea of separation of forwarding and control planes, the next characteristic of SDN is the simplification of network devices, which are then controlled by a centralised system that runs management and control software. Instead of hundreds of thousands of lines of complicated control plane software running on the device, allowing the device to behave autonomously, that software is removed from the device and placed in a centralised controller. This software-based controller may then manage the network based on higher-level policies. The controller provides primitive instructions to the simplified devices when appropriate in order to allow them to make fast decisions about how to deal with incoming packets.

The centralised software-based controller in SDN provides an open interface on the controller to allow for automated control of the network. In the context of SDN, the terms northbound and southbound are often used to distinguish whether the interface is to the applications or to the devices. These terms derive from the fact that in most diagrams the applications are depicted above (i.e. to the north of) the controller while devices are depicted below (i.e. to the south of) the controller. An example of a southbound API (Application Programming Interface) is the OpenFlow interface that the controller uses to program the network devices (McKeown et al., 2008). The controller offers a northbound API, allowing software applications to be plugged into the controller, and thereby allowing that software to provide the algorithms and protocols that can run the network efficiently. These applications can quickly and dynamically make network changes as the need arises.

The northbound API of the controller is intended to provide an abstraction of the network devices and topology. There are three key benefits that the application developer should derive from the northbound API: (1) it converts to a syntax that is more familiar to developers (e.g. REST or JSON); (2) it provides abstraction of the network topology and network layer allowing the application programmer to deal with the network as a whole rather than individual nodes; and (3) it provides abstraction of the network protocols themselves, hiding the application developer from the details of OpenFlow or BGP. In this way, applications can be developed that work over a wide array of manufacturers' equipment that may differ substantially in their implementation details.

### **2.3. OpenFlow and SDN controllers**

OpenFlow is an early protocol specification that describes the communication between OpenFlow switches and an OpenFlow controller. Historically, the term SDN did not come into use until a year after OpenFlow made its appearance in 2008. The OpenFlow protocol defines the specific messages and message formats exchanged between controller (control plane) and device (data plane).

The OpenFlow behaviour specifies how the device should react in various situations, and how it should respond to commands from the controller. The protocol defines two switch components:

- (1) A *flow table* that resides on the switch and performs packet lookup. The fields in each packet are compared to the flow table looking for a match. If a match between the packet headers and any entry of the flow table was found, then an action would be taken by the switch, depending on the found match. If there is no match, then the traffic is sent to the controller.
- (2) A *secure channel* by which the switch communicates with the external controller.

Two mandatory actions in OpenFlow protocol specification are forwarding the packet and dropping it. Forwarding could be to all interfaces (except the incoming interface), to the controller, to the switch's local network stack, to the interface specified by the table flow entry, or to the input port. There is an optional possible forwarding action specified in the OpenFlow protocol, which is to forward the packet in the same way as a normal switch would do, using the spanning tree algorithm. A flow entry with no specified action indicates that all matching packets should be dropped.

Apart from mandatory actions, the OpenFlow protocol specification defines optional actions, including the *Modify* action, whereby the switch may modify various packet header values such as the VLAN ID or the destination IP address. Another optional action is the *Enqueue* action, which sends the packet through a queue attached to a port. OpenFlow switches listen by default to a control port, through which a program called *dpctl* can communicate with the switch even in the absence of a controller. The *dpctl* program allows for performing operations such as inspecting flow table entries and modifying flows.

The OpenFlow specification includes details on metering, traffic monitoring, control channel encryption, handling control messages from multiple controllers, and many other details that can be found in the website of Open Network Foundation (Foundation, 2018).

Other SDN control architectures come from either research community, network vendors, or from the open source community. Among the different SDN controllers that have been introduced, few of the most popular controllers are: NOX/POX, Ryu, Floodlight, Pyretic, Frenetic and Provera. Considerations when choosing a particular controller include the programming language that the controller is written in (which can affect performance), the learning curve (how difficult is it to learn to write policies), the user base and community support, and the focus area of the controller.

#### **2.4. How can SDN help?**

As mentioned earlier, SDN separates the control plane from the data plane, providing the required abstraction of low-level layers into a logical view that can be understood and programmed by network developers. Providing an access into the configuration of network hardware through software programming is essential to allow users to manage their networks via high-level applications that are developed for them by third-party developers. Alternatively, users can outsource network configuration and management to service providers. Viewing the target management functions of each possible application as a separate control *slice* of the home network, trusted third parties can programmatically control different slices to better manage different functions, such as WiFi configuration, improving routing and implementing access control (e.g. configure WiFi channel and power to minimize interference and/or set parental controls).

Several other researchers have previously identified the need for applications and services within the home to cope with increasing complexity and heterogeneity. Few works suggested solutions that are independent of the SDN concept, such as creating new and separate operating system for the home in which users deal with applications and high-level policies to deal with integration and management of their network (Dixon et al., 2010) or using an OSGI (Open Service Gateway Initiative)-based framework to install applications on a residential gateway (Valtchev & Frankov,

2002). However, most of the recent works rely on the SDN technology, and particularly the OpenFlow-based solutions to address the problem of network management. This is the main focus of this article. Aside from the core management functions, and as a subset of those functions, significant work has been done to automate detection and diagnosis of faults in home networks, and to define the appropriate interaction and interfaces between the users and tools to manage and configure the home network (Agarwal et al., 2009).

### 3. Method

In this section, we present the exact steps we followed to select the surveyed papers on SDN in home networks. We explain the method in some detail to make sure it is clear and reproducible. Because the literature on SDN is quite vast, we focus on the most important keyword that distinguishes our target works from all other works on SDN; i.e. home or residential networks. No other restrictions are put on the search. We also limit our scope to the English literature.

Our search for target articles was conducted against four digital databases: (1) the IEEE Xplore library of technical literature in engineering and technology; (2) the ACM digital library on computing and information technology; (3) the ScienceDirect database of science, technical and medical journal articles; and (4) the Wiley online library, indexing cross-disciplinary research in life, health and physical sciences, social science, and the humanities. This selection of databases covers the most important, authentic and comprehensive technical sources. We also tried Springer Link as well as Taylor & Francis Online databases, but no results were found with respect to our search target.

We performed the process of study selection as follows. First, we searched the source databases using a specific query string that contains our target keywords. Then, the duplicates among different databases were removed. After that, we filtered the articles based on the abstract. Finally, few duplicate as well as irrelevant articles were excluded during the full-text reading of the screened articles from the first steps. We applied the same eligibility criteria over all screening iterations, which is to include any English work that reviews, proposes or discusses the use of SDN in home networking for any possible purpose or way.

The search was performed at the end of November 2017. We used a mix of keywords that contained 'home', 'residential', 'software defined networking', 'software defined networks', 'SDN' and 'openflow' with certain search operators to make sure that either 'home' or "residential" appears in the title, and at least one of the other keywords appears anywhere in the text.

### 4. Results

The initial query search resulted in 65 articles: 40 from IEEE Xplore, 20 from ACM library, 4 from ScienceDirect and only one result from Wiley online library, over the span from 2010 to 2017. Five articles were duplicates, where the same article resulted from more than one library databases or the same work was published in more than one venue (e.g. a proceedings and a journal). After scanning the abstracts and then reading the full-text, 18 more articles were excluded, resulting in 42 articles included in the final set. Those papers were studied for the purpose of mapping the current research on software defined home networking and find the general trends and directions in this emerging subfield.

The majority of the surveyed articles (35/42 articles) focus on special themes in the context of managing home networks, while the rest (7/42) address the problem of home network management in a generic perspective without focusing on a particular target application. Among the first group, the most popular theme is the Quality of Experience (QoE) for home network users (11/42 articles), in which the proposals mostly address the problems of bandwidth allocation and adaptive video streaming. Other groups of articles propose SDN to manage IoT smart-home devices (5/42), secure home networks (4/42), manage the usage of Internet (4/42), manage wireless access points (4/42), slice home networks (3/42), manage heterogeneous networks (1/42), automatically

configure home networks (1/42), troubleshoot home networks (1/42) or address the problem of multi-home networking (1/42). The breakdown of these categories is shown in Figure 2.

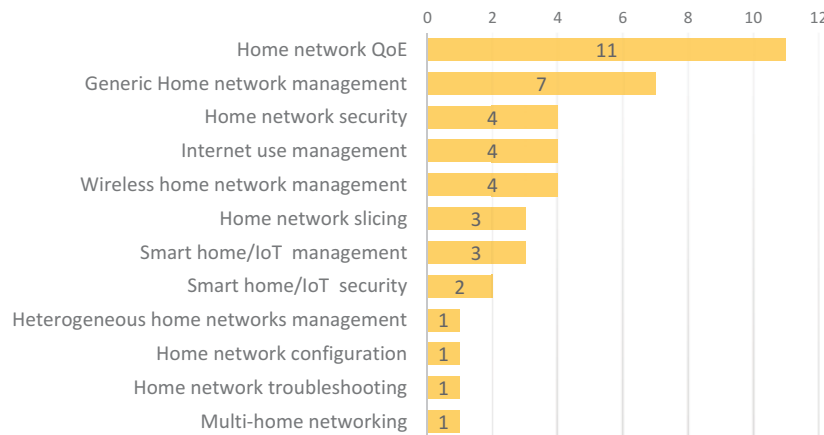
#### 4.1. A taxonomy of the surveyed works

Based on the resulting categories in Figure 3 and the observed patterns and trends in the surveyed research papers, we have derived a basic taxonomy of all works on the subject, shown in Figure 3. We can distinguish between two overall trends in the surveyed works, one is general and the other is specialised. In the following subsections, we briefly list those works according to their category. A more detailed summary of all mentioned works can be found in the (Appendix).

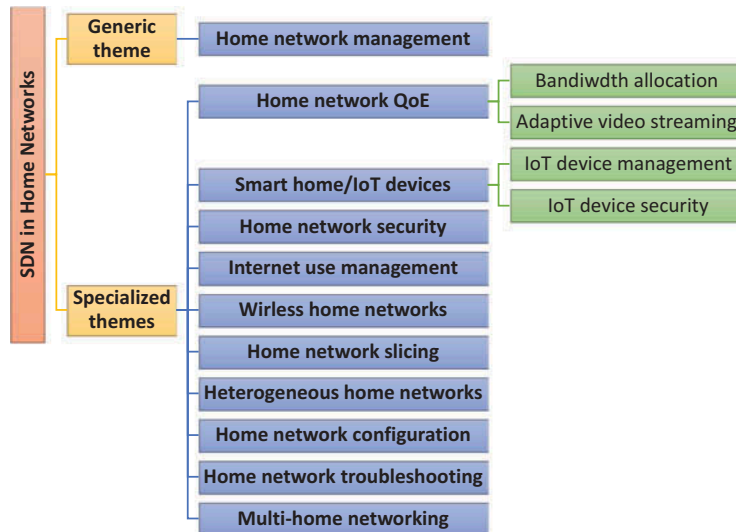
##### 4.1.1. Generic theme

Apart from the works that focus on a specific aspect of managing home networks, such as bandwidth allocation or security, several articles introduce their own approach of exploiting SDN in home networking, from a general perspective. Two of the first works in this category were developed as part of the Homework project (The University of Nottingham, 2012), and aimed at redesigning exiting home-network infrastructure (i.e. routers) based on the concepts of SDN to provide the user with better understanding and control as well as novel interfaces (Mortier et al., 2011, 2012). The authors in (Chetty & Feamster, 2012) take the home network as a case study to discuss how SDN can be used to refactor current networks and provide users with the correct level

**Figure 2. Breakdown of survey results categorising the target application.**



**Figure 3. A taxonomy of works on software defined home networks.**



of network visibility and actionable information. The concept of virtualisation is suggested in the remaining works of this generic category (Boussard et al., 2014; Dillon & Winters, 2014; Flores Moyano, Fernández, Bellido, & González, 2017; Moyano, Cambroner, & Triana, 2017). These four works differ in their proposed architectures, but agree on virtualising the home network and delegating the management and control of the network to someone in the cloud, most probably the Internet Service Provider (ISP). This aims to remove the management burden from the user while providing the usability of the network.

#### 4.1.2. Specialised themes

In this category, we can find few different themes. The general purpose is still to control and manage the home network using ideas and tools from the SDN paradigm, but the emphasis is put on a particular aspect of home networking in each work. We could recognize several specialised themes and summarised them into 10 different subcategories, some of which have only one paper each, but the theme is distinct enough to be highlighted and pointed out for further study and research.

The most popular subject in this category is the QoS and quality of user experience (QoE) when using home network applications (Abuteir, Fladenmuller, & Fourmaux, 2016; Agapiou, Papafili, & Agapiou, 2014; Bakhshi & Ghita, 2016; Bozkurt & Benson, 2016; Eghbali & Wong, 2015; Gharakheili, Bass, Exton, & Sivaraman, 2014; Jang, Huang, & Yeh, 2016; Kumar, Gharakheili, & Sivaraman, 2013; Moyano et al., 2017; Trajkovska, Aeschlimann, Marti, Bohnert, & Salvachúa, 2014; Yang, Wang, Nguyen, & Lu, 2016). The target application in these works is generally multimedia and video streaming, and the aim is to optimize bandwidth allocation for different network applications to improve the user experience. This optimisation is mostly based on the user preferences or profile, but can also be derived from dynamic traffic shaping based on collected traffic statistics (Abuteir, Fladenmuller, & Fourmaux, 2016), automatic identification of applications (Yang, Wang, Nguyen, & Lu, 2016) or a proposed bandwidth allocation algorithm (Jang, Huang, & Yeh, 2016). Most of the works enable the ISP of controlling the service quality from the cloud, though few works depend on local solution using in-home SDN controller (Abuteir et al., 2016), (Bozkurt & Benson, 2016), (Bakhshi & Ghita, 2016). One work also proposes a novel pricing scheme for ISPs, who can implement time-dependent hybrid pricing through SDN APIs (Eghbali & Wong, 2015).

Another distinct theme in this category is to address the issues related to IoT devices, in the context of smart home (Hernando, Fariña, Triana, Piñar, & Cambroner, 2017; Kim & Lee, 2015; Nobakht, Sivaraman, & Boreli, 2016; Sivaraman, Gharakheili, Vishwanath, Boreli, & Mehani, 2015; Xu, Wang, Wei, Song, & Mao, 2016). This perspective is unique and new to home networking, but its relevance is increasing in modern homes with the rise of the IoT paradigm. All network-enabled devices in the home are eventually forming an internet of things, and their management can consequently be considered a networking problem; hence, the SDN comes to mind. Within the papers on IoT home devices, some works focus on the problem of managing IoT devices, such as finding a device fault easily (Kim & Lee, 2015), integrating the heterogeneous network devices in smart home environments (Xu, Wang, Wei, Song, & Mao, 2016), and offering a portfolio of IoT-related functions to home users (Hernando, Fariña, Triana, Piñar, & Cambroner, 2017). Another focus point is to propose solutions for smart home and IoT device security (Nobakht et al., 2016, Sivaraman, Gharakheili, Vishwanath, Boreli, & Mehani, 2015).

Apart from IoT, targeting the application of home network security is also a common theme. One of the earliest works in the complete set of the surveyed papers proposed that users out-source the management tasks related to security to a third party controller who has the required expertise and capacity to monitor coordinated activities over the Internet (Feamster, 2010). Another work proposes a multi-stage attack mitigation mechanism for home networks using SDN (Luo, Wu, Li, & Guo, 2016). A home-level security proxy solution for the video conferencing



applications (as a case study) is proposed in (Taylor, Shue, & Najd, 2016). Finally, a community-based crowdsourced home cyber-security system is proposed in (Stewart, Vasu, & Keller, 2017).

Because the caps of Internet usage is an increasing concern for home users, several works specifically address the problem of managing Internet use through the SDN architecture (Chetty et al., 2015; Gharakheili, Exton, Sivaraman, Matthews, & Russell, 2015; Kim, Sundaresan, Chetty, Feamster, & Edwards, 2011; Yiakoumis et al., 2012). An early work (Kim et al., 2011) demonstrates a system to collect usage statistics and reports them to a central controller, which displays usage information. The controller allows users to specify policies and enforces them, where policies dictate how different people, devices, and applications should consume the usage cap. The other works depend either on the ISP, where the users are allowed to choose the relative priority of their applications, and signal their preference to the ISP (Yiakoumis et al., 2012), or allow a third party to control the Internet traffic usage (Gharakheili, Exton, Sivaraman, Matthews, & Russell, 2015), (Chetty et al., 2015).

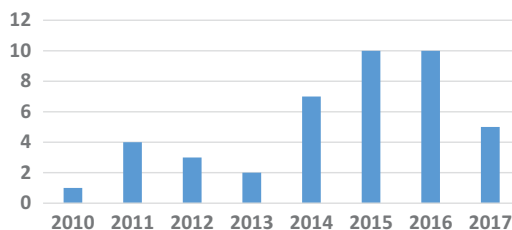
Another group of papers address the specific issues arising from managing home WiFi access points (Patro & Banerjee, 2015a, 2015b; Schulz-Zander, Mayer, Ciobotaru, Schmid, & Feldmann, 2015), or in general all multi-technology wireless network devices (Gallo, Kosek-Szott, Szott, & Tinnirello, 2016). Few papers adopt the concept of network slicing (Fratczak, Broadbent, Georgopoulos, & Race, 2013; Wang, Wu, Chen, Wang, & Li, 2014; Yiakoumis, Yap, Katti, Parulkar, & McKeown, 2011). Network slicing is a promising technique that creates different slices over the same physical home network, so that each slice is independently controllable and can be isolated for different services. The management of slices may be assigned to a third party.

Finally, the last four papers in our collection are directed toward four special target applications. The first work proposes the instrumentation of home networks to enable their troubleshooting (Calvert et al., 2011). This work presents the design requirements of a general-purpose home network logging platform that can record events supporting troubleshooting services for home network users. A second work discusses the idea of multi-home networking (Jo, Lee, & Kim, 2014), enabling on-demand provisioning of networked multi-home multimedia applications using SDN-based in-home consumer electronic devices. The automatic configuration of home networks is also addressed in (Lee, Kim, & Lee, 2015), which proposes a method where SDN controller performs auto-recognition and registration of home devices, then manages home devices according to the home network connection state. The final work addresses the problem of heterogeneity in home networks, and evaluates the ability of OpenFlow-enabled switches to manage heterogeneous home networks by utilising redundant links for flow rerouting and performing link switching between wired and wireless technologies both under normal conditions and in case of link failures (Soetens, Famaey, Verstappen, & Latré, 2015).

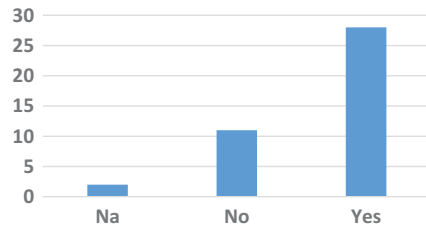
#### 4.2. Basic statistics

This subsection presents few basic statistics to highlight a couple of points. The first one is shown in Figure 4, and illustrates the number of published works on using SDN in home networks by the year. Despite the slight regression in 2017, the last 3 years witnessed an increased interest of researchers in the topic of software-defined home networking. Another interesting observation is the extent to which the proposed solutions rely on entities outside the home to manage the home

Figure 4. Number of surveyed papers by year.



**Figure 5. Classification of works according to whether they are based on a third party or cloud.**



network. Figure 5 compares the number of proposals that are based on a third party or the cloud (e.g. an ISP) to the number of proposals that manage the home network locally within the home itself without outsourcing any task to the cloud. 'Na' in the figure refers to the cases where this detail is not available. Finally, Figure 6 depicts the number of works based on the OpenFlow protocol. As expected, excluding a few works where there are no exact implementation details, OpenFlow is used in most of the works. This comes as no surprise for the most popular open protocol in SDN implementations.

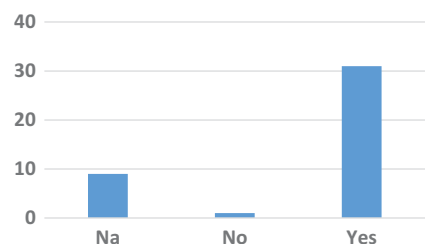
### 5. Discussion

The purpose of this article is to explore the available works on using SDN in the realm of home networks. After a couple years of research into the paradigm of SDN that commenced circa 2008, researchers soon realised the value of the new idea in contexts other than data centers and large enterprise networks. Indeed, the challenges of modern home networks and the complexity of their management push towards new approaches and reminds every one of the flexibility and power that SDN can bring in. The separation of control from data makes it possible to isolate the low-level details of how home network devices work and provide the home user (or a third party for that matter) with a clean interface to control network operation exploiting the new programmability of networks. Many network management functions that are not possible to perform in current home networks by average home users become feasible, and easy to perform, with the help of SDN.

Based on the results of our survey, a couple of points may be worth highlighting in this discussion. First, it is apparent from the derived taxonomy that many individual tasks of network management can be the target of an SDN-based solution, such as Internet usage, security and QoE. Most of the surveyed works focused on these tasks and produced different architectures and prototypes to prove the concept of their design and demonstrate its implementation. Although these works have the SDN basis in common, they are independent of each other and, most probably, incompatible. Each one alone is also incomprehensive in terms of the whole range of network management tasks. This leads to the need for further studies to analyse, evaluate and combine these solutions into a unified framework, a sort of one-stop product for software defined home networking. We might eventually end with few such products, but the potential to integrate many of the proposed ideas is great.

Second, many solutions aim to put the control in the hands of the home user in managing their home networks. Whatever was the underpinning mechanism, all solutions would need to interface with the user at the front-end. The role of the interface is crucial; it should make various

**Figure 6. Classification of works according to whether they are based on OpenFlow.**



functionalities and information on the underlying network visible to the user, and allow the user to make changes in response to those information. As pointed out in (Chetty & Feamster, 2012), this raises questions on how to expose that kind of new functionality to the users using intuitive interfaces that improve their awareness of the network status and enable them of taking actions. For example, the downstream speed of the Internet broadband connection might be represented by the width of a pipe, and packet loss might be shown as certain traffic not making it all the way through the pipe. Slides and icons can represent various devices and dropdown lists can present available actions...etc. That being said, it is also important to remember that while a novice user needs understand no details, an expert user might gain additional insight from knowing the underlying details, and hence exposing various levels of visibility may be required.

Finally, an important point to notice is that most of the works suggest the involvement of a cloud-based, third party (such as the ISP) in the management of the virtualised home network. As pointed in (Chetty & Feamster, 2012) again, determining what information should be collected and presented to the operator is an area for future work. The challenge here is to balance the home user's privacy with the need for an ISP operator to see the configuration, topology, and devices on the home network. From a security perspective, exposure to external entities may also increase the attack surface on the home network, as more channels and more information are open to outside the perimeter of the home network.

## 6. Conclusion

In this article, we have surveyed the state-of-the-art in applying the concept of SDN to the problem of managing home networks. Modern home users are quite familiar with the concept of programmability; the modern lifestyle involves a lot of interaction with programmable devices (e.g. computers and smartphones) that can be controlled by applications, using intuitive and attractive interfaces. SDN is a powerful paradigm that introduces the same idea of programmability to networked devices in the home, so that home networks can be controlled and managed through application-level interfaces. This idea has been investigated in a number of works by now. The purpose of this article was to scan, taxonomised and summarize these initial proposals. Basic statistics have been derived and few important points have been discussed. To the best of our knowledge, this is the first dedicated survey of using SDN in home network management, and we hope that it can provide the readers with an entry point to the emerging subfield of software defined home networking.

### Acknowledgements

The authors would like to thank University Teknikal Malaysia Melaka and INSFORNET Research Group for their incredible support by providing facilities to conduct the study.

### Funding

The authors received no direct funding for this research.

### Author details

Abdalkrim M. Alshnta<sup>1</sup>  
E-mail: [kshnta@gmail.com](mailto:kshnta@gmail.com)  
Mohd Faizal Abdollah<sup>1</sup>  
E-mail: [faizalabdollah@utem.edu.my](mailto:faizalabdollah@utem.edu.my)  
Ahmed Al-Haiqi<sup>2</sup>  
E-mail: [ahmedmubarak@uniten.edu.my](mailto:ahmedmubarak@uniten.edu.my)  
ORCID ID: <http://orcid.org/0000-0001-9181-4699>  
<sup>1</sup> Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia.  
<sup>2</sup> Department of Electronics and Communication Engineering, Universiti Tenaga Nasional, Kajang, Malaysia.

### Citation information

Cite this article as: SDN in the home: A survey of home network solutions using Software Defined Networking, Abdalkrim M. Alshnta, Mohd Faizal Abdollah & Ahmed Al-Haiqi, *Cogent Engineering* (2018), 5: 1469949.

### References

- Abuteir, R. M., Fladenmuller, A., & Fourmaux, O. (2016). An SDN approach to adaptive video streaming in wireless home networks. In *2016 International wireless communications and mobile computing conference (IWCMC)* (pp. 321–326).
- Agapiou, G., Papafili, I., & Agapiou, S. (2014). The role of SDN and NFV for dynamic bandwidth allocation and QoE adaptation of video applications in home networks. In *2014 Euro med telco conference (EMTC)* (pp. 1–4).
- Agarwal, B., Bhagwan, R., Das, T., Eswaran, S., Padmanabhan, V. N., & Voelker, G. M. (2009). NetPrints: Diagnosing home network misconfigurations using shared knowledge. *NSDI*, 9, 349–364.
- Bakhshi, T., & Ghita, B. (2016). User-centric traffic optimization in residential software defined networks. In *2016 23rd International conference on telecommunications (ICT)* (pp. 1–6).
- BeagleBoard.org - black. [Online]. Retrieved November 30, 2017 from <https://beagleboard.org/black>
- Boussard, M., Bui, D. T., Douville, R., Le Sauze, N., Noirie, L., Peloso, P., Varloot, R., & Vigoureux, M. (2014). The majord'home: A SDN approach to let isps manage and extend their customers'home networks. In *10th International conference on network and service management (CNSM) and workshop* (pp. 430–433).
- Bozkurt, I. N., & Benson, T. (2016). Contextual router: Advancing experience oriented networking to the

- home. In *Proceedings of the symposium on SDN research* (p. 15: 1–15:7).
- Calvert, K. L., Edwards, W. K., Feamster, N., Grinter, R. E., Deng, Y., & Zhou, X. (2011, January). Instrumenting home networks. *SIGCOMM computation communicable reviews*, 41(1), 84–89. doi:10.1145/1925861
- Chetty, M., & Feamster, N. (2012, Jun). Refactoring network infrastructure to improve manageability: A case study of home networking. *SIGCOMM computation communicable reviews*, 42(3), 54–61. doi:10.1145/2317307
- Chetty, M., Haslem, D., Baird, A., Ofoha, U., Sumner, B., & Grinter, R. (2011). Why is my internet slow?: Making network speeds visible. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 1889–1898).
- Chetty, M., Kim, H., Sundaresan, S., Burnett, S., Feamster, N., & Edwards, W. K. (2015). uCap: An internet data management tool for the home. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (pp. 3093–3102).
- Cisco. Snort - network intrusion detection & prevention system. [Online]. Retrieved Nov 30, 2017 from <https://www.snort.org/>
- Dillon, M., & Winters, T. (2014, November). Virtualization of home network gateways. *Computer (Long Beach California)*, 47(11), 62–65.
- Dixon, C., Mahajan, R., Agarwal, S., Brush, A. J., Lee, B., Saroiu, S., & Bahl, V. (2010). The home needs an operating system (and an app store). In *Proceedings of the 9th ACM SIGCOMM workshop on hot topics in networks* (p. 18).
- Edwards, W. K., Grinter, R. E., Mahajan, R., & Wetherall, D. (2011). Advancing the state of home networking. *Communicable ACM*, 54(6), 62–71. doi:10.1145/1953122
- Eghbali, H., & Wong, V. W. S. (2015). Bandwidth allocation and pricing for SDN-enabled home networks. In *2015 IEEE international conference on communications (ICC)* (pp. 5342–5347).
- The European Commission DG CONNECT in FP7. Home - UNIFY project. [Online]. Retrieved Nov 28, 2017 from <http://www.fp7-unify.eu/>
- Feamster, N. (2010). Outsourcing home network security. In *Proceedings of the 2010 ACM SIGCOMM workshop on home networks* (pp. 37–42).
- Feamster, N., Rexford, J., & Zegura, E. (2014). The road to SDN: An intellectual history of programmable networks. *ACM SIGCOMM Computation Communicable Reviews*, 44(2), 87–98. doi:10.1145/2602204.2602219
- Ffmpeg. [Online]. Retrieved November 29, 2017 from <https://www.ffmpeg.org/>
- Flores Moyano, R., Fernández, D., Bellido, L., & González, C. (2017). A software-defined networking approach to improve service provision in residential networks. *International Journal Network Managed*. doi:10.1002/nem.1984
- Foundation, O. N. Open networking foundation is an operator led consortium leveraging SDN, NFV and cloud technologies to transform operator networks and business models. [Online]. Retrieved Apr 01, 2018 from <https://www.opennetworking.org/>
- Fratczak, T., Broadbent, M., Georgopoulos, P., & Race, N. (2013). HomeVisor: Adapting home network environments. In *2013 Second European workshop on software defined networks* (pp. 32–37).
- Gallo, P., Kosek-Szott, K., Szott, S., & Tinnirello, I. (2016). SDN@ home: A method for controlling future wireless home networks. *IEEE Communicable Magazine*, 54(5), 123–131. doi:10.1109/MCOM.2016.7470946
- Gharakheili, H. H., Bass, J., Exton, L., & Sivaraman, V. (2014). Personalizing the home network experience using cloud-based SDN. In *Proceeding of IEEE International symposium on a world of wireless, mobile and multimedia networks 2014* (pp. 1–6).
- Gharakheili, H. H., Exton, L., Sivaraman, V., Matthews, J., & Russell, C. (2015). Third-party customization of residential Internet sharing using SDN. In *2015 International telecommunication networks and applications conference (ITNAC)* (pp. 214–219).
- GitHub - noxrepo/nox. (2017). NOX network control platform. [Online]. Retrieved from <https://github.com/noxrepo/nox>
- Coran, P., Black, C., & Culver, T. (2016). *Software defined networks: A comprehensive approach*. Cambridge, MA: Morgan Kaufmann.
- Grinter, R. E., Greenhalgh, C., Benford, S., Edwards, W. K., Chetty, M., Poole, E. S., ... Rodden, T. (2009). The ins and outs of home networking: The case for useful and usable domestic networking. *ACM Transactions Computation Interact*, 16(2), 8. doi:10.1145/1534903
- Haque, I. T., & Abu-Ghazaleh, N. (2016). Wireless software defined networking: A survey and taxonomy. *IEEE Communicable Survey Tutorials*, 18(4), 2713–2737. doi:10.1109/COMST.2016.2571118
- Hernando, A. B. G., Fariña, A. D. S., Triana, L. B., Piñar, F. J. R., & Cambroner, D. F. (2017). Virtualization of residential IoT functionality by using NFV and SDN. In *2017 IEEE international conference on consumer electronics (ICCE)* (pp. 86–87).
- Jang, H.-C., Huang, C.-W., & Yeh, F.-K. (2016). Design a bandwidth allocation framework for SDN based smart home. In *2016 IEEE 7th annual information technology, electronics and mobile communication conference (IEMCON)* (pp. 1–6).
- Jo, J., Lee, S., & Kim, J. W. (2014, August). Software-defined home networking devices for multi-home visual sharing. *IEEE Transactions Consum Electronic*, 60(3), 534–539. doi:10.1109/TCE.2014.6937340
- Kim, H., Sundaresan, S., Chetty, M., Feamster, N., & Edwards, W. K. (2011). Communicating with caps: Managing usage caps in home networks. In *Proceedings of the ACM SIGCOMM 2011 conference* (pp. 470–471).
- Kim, Y., & Lee, Y. (2015). Automatic generation of social relationships between internet of things in smart home using SDN-based home cloud. In *2015 IEEE 29th International conference on advanced information networking and applications workshops* (pp. 662–667).
- Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmalky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings IEEE*, 103(1), 14–76. doi:10.1109/JPROC.2014.2371999
- Kumar, H., Gharakheili, H. H., & Sivaraman, V. (2013). User control of quality of experience in home networks using SDN. In *2013 IEEE International conference on advanced networks and telecommunications systems (ANTS)* (pp. 1–6).
- Lee, M., Kim, Y., & Lee, Y. (2015). A home cloud-based home network auto-configuration using SDN. In *2015 IEEE 12th International conference on networking, sensing and control* (pp. 444–449).
- Luo, S., Wu, J., Li, J., & Guo, L. (2016, May). A multi-stage attack mitigation mechanism for software-defined home networks. *IEEE Transactions Consum Electronic*, 62(2), 200–207. doi:10.1109/TCE.2016.7514720

- McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., ... Turner, J. (2008). OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Computation Communicable Review*, 38(2), 69–74. doi:10.1145/1355734
- Monsanto, C., Reich, J., Foster, N., Rexford, J., & Walker, D. (2013). Composing software defined networks. *NSDI*, 13, 1–13.
- Mortier, R., Bedwell, B., Glover, K., Lodge, T., Rodden, T., Rotsos, C., ... Sventek, J. (2011). Supporting novel home network management interfaces with open-flow and NOX. In *Proceedings of the ACM SIGCOMM 2011 Conference* (pp. 464–465).
- Mortier, R., Rodden, T., Lodge, T., McAuley, D., Rotsos, C., Moore, A. W., Kolioussis, A. & Sventek, J. (2012). Control and understanding: Owning your home network. In *2012 Fourth International conference on communication systems and networks (COMSNETS 2012)* (pp. 1–10).
- Moyano, R. F., Cambroner, D. F., & Triana, L. B. (2017). A user-centric (SDN) management architecture for NFV-based residential networks. *Computation Standards Interfaces*, 54(Part 4), 279–292. doi:10.1016/j.csi.2017.01.010
- Moyano, R. F., Fernández, D., Bellido, L., Merayo, N., Aguado, J. C., & De Miguel, I. (2017). NFV-based QoS provision for software defined optical access and residential networks. In *2017 IEEE/ACM 25th International symposium on quality of service (IWQoS)* (pp. 1–5).
- ns-3. [Online]. Retrieved November 29, 2017 from <https://www.nsnam.org/>
- Nobakht, M., Sivaraman, V., & Boreli, R. (2016). A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow. In *2016 11th International conference on availability, reliability and security (ARES)* (pp. 147–156).
- Nunes, B. A. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communicable Survey Tutorials*, 16(3), 1617–1634. doi:10.1109/SURV.2014.012214.00180
- OpenWrt. [Online]. Retrieved November 29, 2017 from <https://openwrt.org/>
- Open vSwitch. 2017. [Online]. Retrieved November 20, 2017 from <http://openvswitch.org/>
- Patro, A., & Banerjee, S. (2014). COAP: A software-defined approach for home WLAN management through an Open API. In *Proceedings of the 9th ACM workshop on mobility in the evolving internet architecture* (pp. 31–36).
- Patro, A., & Banerjee, S. (2015a, January). COAP: A software-defined approach for home WLAN management through an Open API. *SIGMOBILE Mobile Computation Communicable Reviews*, 18(3), 32–40. doi:10.1145/2721896
- Patro, A., & Banerjee, S. (2015b). Outsourcing coordination and management of home wireless access points through an open API. In *2015 IEEE conference on computer communications (INFOCOM)* (pp. 1454–1462).
- Project BISmark (Broadband internet service benchmark). (2017). [Online]. Retrieved November 19, 2017 from <http://projectbismark.net/>
- Project Floodlight. Floodlight OpenFlow controller-project floodlight. [Online]. Retrieved November 29, 2017 from <http://www.projectfloodlight.org/floodlight/>
- Ryu SDN Framework Community. (2017). Ryu SDN framework. [Online]. Retrieved November 27, 2017 from <https://osrg.github.io/ryu/>
- Schulz-Zander, J., Mayer, C., Ciobotaru, B., Schmid, S., & Feldmann, A. (2015). OpenSDWN: Programmatic control over home and enterprise WiFi,” in *Proceedings of the 1st ACM SIGCOMM symposium on software defined networking research* (p. 16: 1–16:12).
- Sherwood, R., Gibb, G., Yap, K. K., Appenzeller, G., Casado, M., McKeown, N., ... Parulkar, G. (2009). Flowvisor: A network virtualization layer. *OpenFlow Switch Consortium, Technical Reports*, 1, 132.
- Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-level security and privacy control for smart-home IoT devices. In *2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob)* (pp. 163–167).
- Soetens, N., Famaey, J., Verstappen, M., & Latré, S. (2015). SDN-based management of heterogeneous home networks. In *2015 11th International conference on network and service management (CNSM)* (pp. 402–405).
- Stewart, C. E., Vasu, A. M., & Keller, E. (2017). CommunityGuard: A crowdsourced home cybersecurity system. In *Proceedings of the ACM International workshop on security in software defined networks & network function virtualization* (pp. 1–6).
- Taylor, C. R., Shue, C. A., & Najd, M. E. (2016). Whole home proxies: Bringing enterprise-grade security to residential networks. In *2016 IEEE International conference on communications (ICC)* (pp. 1–6).
- Trajkowska, I., Aeschlimann, P., Marti, C., Bohnert, T. M., & Salvachúa, J. (2014). SDN enabled QoS provision for online streaming services in residential ISP networks. In *2014 IEEE International conference on consumer electronics - taiwan* (pp. 33–34).
- The University of Nottingham. (2012). Homework – User-centred home networking. [Online]. Retrieved November 20, 2017 from <http://homenetworks.ac.uk/>
- Valtchev, D., & Frankov, I. (2002). Service gateway architecture for a smart home. *IEEE Communicable Magazine*, 40(4), 126–132. doi:10.1109/35.995862
- Wang, S., Wu, X., Chen, H., Wang, Y., & Li, D. (2014). An optimal slicing strategy for SDN based smart home network. In *2014 International conference on smart computing* (pp. 118–122).
- Xu, K., Wang, X., Wei, W., Song, H., & Mao, B. (2016, May). Toward software defined smart home. *IEEE Communicable Magazine*, 54(5), 116–122. doi:10.1109/MCOM.2016.7470945
- Yang, H., Wang, X., Nguyen, C.-T., & Lu, S. (2016). Conan: Content-aware access network flow scheduling to improve QoE of home users. In *Proceedings of the 2016 ACM SIGCOMM conference* (pp. 575–576).
- Yiakoumis, Y., Katti, S., Huang, T.-Y., McKeown, N., Yap, -K.-K., & Johari, R. (2012). Putting home users in charge of their network. In *Proceedings of the 2012 ACM conference on ubiquitous computing* (pp. 1114–1119).
- Yiakoumis, Y., Yap, -K.-K., Katti, S., Parulkar, G., & McKeown, N. (2011). Slicing home networks. In *Proceedings of the 2Nd ACM SIGCOMM workshop on home networks* (pp. 1–6).

### Appendix: A summary of the complete list of surveyed articles, sorted by year of publication

Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Fearmster, 2010)	Outsourcing Home Network Security	2010	Proposes that users outsource the management tasks related to security to a third party controller who has the required expertise and capacity to monitor coordinated activities over the Internet and can take necessary actions to protect the user networks through programmable gateways.	Home network security	<ul style="list-style-type: none"> <li>Spam filtering</li> <li>Botnet and malware detection</li> </ul>	Yes	System proposal at the conceptual level	Yes
(Kim et al., 2011)	Communicating with Caps: Managing Usage Caps in Home Networks	2011	Demonstrates a system that can monitor and manage Internet usage caps. BISMark firmware runs on the routers to collect usage statistics and reports them to a central controller, which displays usage information. The controller allows users to specify policies and enforces them. Policies dictate how different people, devices, and applications should consume the usage cap. The controller communicates with the devices using a secure OpenFlow channel.	Internet use management	<ul style="list-style-type: none"> <li>Limiting the usage of a particular application</li> <li>Visualising usage statistics</li> <li>Allowing users within a single household to "trade" caps with one another</li> </ul>	No	System demonstration. The system uses both Kermit (Chetty et al., 2011) at the front end and BISMark (BISMark, 2017) on the gateways.	Yes

(Continued)

(Continued)								
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Calvert et al., 2011)	Instrumenting Home Networks	2011	Discusses the design requirements of a general-purpose home network logging platform that can record events supporting troubleshooting services for home network users. The proposed design can also have other applications such as Internet performance measurement, network security and network troubleshooting and auto-configuration.	Home network troubleshooting	Na	No	Initial prototype data collection system as a proof-of-concept, based on NOX (GitHub—noxrepo/nox, 2017)/OpenFlow. The implemented prototype is called Home Network Data Recorder (HNDR)	Yes
(Yiakouris et al., 2011)	Slicing Home Networks	2011	Proposes the slicing of home networks, which is a mechanism to allow multiple service providers to share a common network and support many policies and business models for cost sharing. The paper also discusses several requirements for slicing: bandwidth and traffic isolation between slices, independent control of each slice, and the ability to modify and improve the behaviour of a slice.	Home network slicing	<ul style="list-style-type: none"> <li>Sharing the physical network</li> <li>Outsourcing network management</li> <li>Customising slices for applications</li> </ul>	Yes	Initial prototype that uses OpenFlow and FlowVisor (Sherwood et al., 2009), a slicing mechanism for OpenFlow networks.	Yes

(Continued)

<b>(Continued)</b>								
<b>Ref.</b>	<b>Title</b>	<b>Year</b>	<b>Summary</b>	<b>Target application</b>	<b>Example use cases</b>	<b>Cloud based*</b>	<b>Tangible output</b>	<b>OF</b>
(Mortier et al., 2011)	Supporting Novel Home Network Management Interfaces with OpenFlow and NOX	2011	Provides a demonstration of management interfaces for a home networking platform that was developed as part of The Homework project (The University of Nottingham, 2012). This project attempted to redesign existing home network infrastructures to better support the needs of home users. The demonstrated platform provides detailed per-flow measurement and management capabilities supporting several novel management interfaces.	Home network management	<ul style="list-style-type: none"> <li>• Displaying per-device per-protocol bandwidth usage</li> <li>• Displaying wireless signal strength, current total bandwidth use and DHCP lease grant activity using LEDs</li> <li>• Managing DHCP allocations</li> <li>• Enabling specific devices to connect to the network as well as limiting access to specified web services, e.g. Facebook</li> </ul>	No	A platform in the form of a small form-factor PC acting as the home router, exposing various APIs. A software runs on top of a standard Linux Ubuntu distribution running Open vSwitch (2017) and NOX.	Yes

(Continued)



(Continued)								
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Mortier et al., 2012)	Control and Understanding: Owning Your Home Network	2012	Similar to (Mortier et al., 2011), investigates the redesign of home routers to exploit the social and physical differences of the home network from the Internet backbone network. Focuses on providing users with understanding of their networks and with control over them. The proposed design of routers enables traffic isolation and accurate measurement from the IP layer. It also provides finer-grained per-flow control via interception of wireless association, DNS resolution, and a platform for building user interfaces.	Home network management	<ul style="list-style-type: none"> <li>Guest board application to enable easy admission of new devices to the home network</li> </ul>	No	A prototype that uses NOX and OpenFlow to provide per-flow control. The presented implementation required modification to the behaviour (but not the wire format) of three standard protocols, DHCP, EAPOL and DNS.	Yes
(Yiakoumis et al., 2012)	Putting Home Users in Charge of their Network	2012	Focuses on the user-ISP interaction and proposes to allow the user to choose the relative priority of their applications, and signal their preference to the ISP using user-agents, which translate high-level user intentions to low-level network semantics.	Internet use management	<ul style="list-style-type: none"> <li>Web-based agent for static provisioning</li> <li>Agent integrated with Skype for low-latency VoIP</li> <li>Interactive agent for on-demand bandwidth for video-streaming</li> </ul>	Yes	A basic prototype to illustrate the main points of the proposed design, especially user intents and how they are mapped to network semantics. The paper refers the reader to (Yiakoumis et al., 2011) for details on the network slicing mechanism.	Na

(Continued)

(Continued)						
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*
(Chetty & Fearmster, 2012)	Refactoring Network Infrastructure to Improve Manageability: A Case Study of Home Networking	2012	Based on the premise that SDN enables the refactoring of the underlying network without compromising existing functionality, this paper explores opportunities for refactoring home network functions to improve system visibility, drawing on examples from existing literature. The authors discuss where current aspects of home networking are too visible or too hidden from users and provide examples of how refactoring network functions can facilitate the design of interfaces that ultimately improve user experience.	Home network management	Refactoring home network to: <ul style="list-style-type: none"> <li>• Simplify network setup, improve visible connections, reduce difficulty of upgrading infrastructure and shift management tasks to third parties</li> <li>• Enable better measurements and improve performance visibility for ISPs</li> <li>• Make policy setup more intuitive by separating policy from mechanism</li> </ul>	Na
						Na

(Continued)

(Continued)								
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Fratczak, Broadbent, Georgopoulos, & Race, 2013)	HomeVisor: Adapting Home Network Environments	2013	Introduces HomeVisor, a home network configuration and management tool, and evaluates its ability to outsource control to an entity outside the home network. This tool relies on the concept of slicing home networks to provide fast and fine-grained home network configuration, quick creation and management of new and existing network slices, and outsourcing control of these slices to other parties.	Home network slicing	<ul style="list-style-type: none"> <li>• Remote home network troubleshooting</li> <li>• Fine-grained configurations</li> <li>• User agnostic and non-application centric approach</li> </ul>	Yes	A prototype for home network management tool (HomeVisor) that uses another OpenFlow-based network slicing tool, FlowVisor. HomeVisor has three main components: 1) web user interface that provides a front-end control interface through which users can manage their network and upload new configurations; 2) network management component that acts as a gateway to the underlying OpenFlow software; and 3) XML API that translates XML-based setups for easy configuration and reconfiguration.	Yes
(Kumar et al., 2013)	User Control of Quality of Experience in Home Networks using SDN	2013	Uses SDN to enable the ISP to expose selected controls to the users for managing quality of service for specific devices and applications in their home networks. The authors develop an architecture and interface for delegation of such control to the user, and demonstrate its value via testbed experiments.	Home network QoE	<ul style="list-style-type: none"> <li>• Video</li> <li>• Web-browsing</li> <li>• Large downloads</li> </ul>	Yes	A prototype for the proposed architecture in the form of a Java GUI by which users can prioritize their devices and applications. The Java application maps these high-level preferences into low-level APIs sent to the ISP, which can slice the access link according to the user's requirements to maintain QoE.	Yes

(Continued)

(Continued)								
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Wang et al., 2014)	An Optimal Slicing Strategy for SDN based Smart Home Network	2014	Discusses slicing strategies for home networks, and compares between several strategies using a prototype implementation. Three types of slicing strategies are evaluated, from which an optimal strategy is derived.	Home network slicing	<ul style="list-style-type: none"> <li>• Application slicing, where applications are prioritised based on user preference or past experience</li> <li>• Location slicing based on the nearby devices in the home network</li> <li>• Bandwidth strategy conducts slicing based on bandwidth requirements</li> </ul>	No	The proposed home network architecture was deployed in the Mininet simulator over VMware Workstation and the latest version of FlowVisor was used to slice the home network.	Yes
(Gharakheili, Bass, Exton, & Sivaraman, 2014)	Personalising the Home Network Experience using Cloud-Based SDN	2014	Proposes to personalize the home network experience, where the network can differentiate users (e.g. parent vs. children computers) and services (e.g. video streaming prioritised over downloading). The authors develop an architecture that includes a cloud-based front-end user interface and SDN-based APIs in the back-end, by which ISPs allow users to customize their home network experience.	Home network QoE	<ul style="list-style-type: none"> <li>• YouTube streaming video quality</li> <li>• Skype video-conferencing experience</li> <li>• Facebook parental control access</li> </ul>	Yes	A prototype of the proposed architecture, which uses a cloud-based GUI and implements the model APIs using Open vSwitch and Floodlight controller. Evaluation experiments use client scripts to generate real traffic.	Yes

(Continued)

<b>(Continued)</b>								
<b>Ref.</b>	<b>Title</b>	<b>Year</b>	<b>Summary</b>	<b>Target application</b>	<b>Example use cases</b>	<b>Cloud based*</b>	<b>Tangible output</b>	<b>OF</b>
(Trajkovska, Aeschlimann, Marti, Bohnert, & Salvachua, 2014)	SDN enabled QoS Provision for Online Streaming Services in Residential Networks	2014	Proposes SDN-based QoS management in residential networks for online streaming services. The authors propose a set of APIs to adjust users QoS via the OpenFlow protocol.	Home network QoE	<ul style="list-style-type: none"> <li>Multimedia streaming service</li> </ul>	Yes	A simulated network to verify the proposed idea using Mininet, where network nodes are connected to an OpenFlow switch running Ryu (Ryu SDN Framework Community, 2017) controller.	Yes
(Jo et al., 2014)	Software-defined Home Networking Devices for Multi-home Visual Sharing	2014	Proposes SDN-based in-home consumer electronic devices that enable on-demand provisioning for protocol-agnostic home networking to serve networked multi-home multimedia applications.	Multi-home networking	<ul style="list-style-type: none"> <li>Inter-home multimedia sharing</li> </ul>	Yes	A prototypic implementation of the proposed CE devices (HomeBox and ControlBox). A HomeBox device is a gateway device to interconnect two home networks by leveraging SDN. The ControlBox configures the gateway HomeBox to support integrating multiple home networks. Few PCs are used to implement the proposed devices.	No

(Continued)

(Continued)								
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Boussard et al., 2014)	The Majord'Home: a SDN Approach to Let ISPs Manage and Extend Their Customers' Home Networks	2014	Proposes an approach to relieve the user from the burden of home network management, by fully virtualising the home network and delegating its management and control to the ISP, while keeping users in control using a simplified interface, through which they express their preferences that are translated into low level configuration instructions. The authors also define the architecture of a software-based Majord'Home solution, which acts as a homes' majordomo.	Home network management	<ul style="list-style-type: none"> <li>• Sharing private TV to watch video from media server of another home as if both devices were located within the same LAN</li> </ul>	Yes	A first prototype for the proposed Majord'Home architecture, the core of which is built on top of many blocks and tools for the various components of the architecture, including Open vSwitch, Open Daylight, and other software frameworks.	Yes
(Agapiou, Papafili, & Agapiou, 2014)	The role of SDN and NFV for dynamic bandwidth allocation and QoS adaptation of video applications in home networks	2014	Analyses the appliances of home networks, such as DSL CPE, for a video service by presenting and describing the various interfaces in the different layers of the UNIFY (The European Commission DG CONNECT in FP7, 2017) architecture from which the benefits and advantages of SDN and NFV can be derived.	Home network QoS	<ul style="list-style-type: none"> <li>• Video streaming in which some packet losses during the play are accepted</li> <li>• HD video with high QoS</li> <li>• Video conference, in which voice is prioritised over video</li> </ul>	Na	Na	Na

(Continued)

<b>(Continued)</b>								
<b>Ref.</b>	<b>Title</b>	<b>Year</b>	<b>Summary</b>	<b>Target application</b>	<b>Example use cases</b>	<b>Cloud based*</b>	<b>Tangible output</b>	<b>OF</b>
(Dillon & Winters, 2014)	Virtualisation of Home Network Gateways	2014	Proposes a virtual gateway that combines SDN with virtualisation to reduce the burden on home network gateways and provide flexibility in handling the increasing demand for device connection and new home services.	Home network management	<ul style="list-style-type: none"> <li>Quality of service (QoS)</li> <li>Failovers</li> <li>M2M communication</li> </ul>	Yes	An implementation of an open source solution that moves the home gateway functions out of the physical hardware into a virtualised gateway in the cloud. OpenFlow switches are used OpenWrt home routing software.	Yes
(Lee et al., 2015)	A Home Cloud-based Home Network Auto-Configuration using SDN	2015	Proposes a new method for the auto-configuration of home networks in home cloud environments based on SDN. SDN controller performs auto-recognition and registration of home devices, then manages home devices according to the home network connection state. In order to achieve this, a home device database is developed, as well as an auto-configuration module that interlocks in an SDN controller.	Home network configuration	<ul style="list-style-type: none"> <li>Home device auto-recognition and management without using a specific standard</li> </ul>	Yes	An evaluation using the Mininet simulator. Independent home cloud server environment is created using OpenDaylight, and Open vSwitch (OVS) is used as the OpenFlow switch. Mininet is used to create several virtual home device nodes and networks.	Yes

(Continued)

(Continued)								
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Kim & Lee, 2015)	Automatic Generation of Social Relationships between Internet of Things in Smart Home using SDN- based Home Cloud	2015	Proposes the concept of social relationships in the context of IoT. The main aim is to find the position of a fault easily, and four social relationships are defined: IoT-IoT, IoT-Network, and IoT-Service and IoT-Physical space relationship. These relationships can be used to discover IoT devices, services and resources are generated automatically by an SDN-based home cloud.	Smart home/IoT management	<ul style="list-style-type: none"> <li>Home IoT fault diagnosis system based on social IoT Relationships</li> <li>Semantic query-based solution service for an IoT device problem</li> </ul>	Yes	A simulation of the automatic generation of relationships using 307 switches and 2007 device nodes. The created relationships are stored as a RDF/XML format, which can be used to fulfil a semantic query or smart home service recommendation.	Yes
(Eghbali & Wong, 2015)	Bandwidth Allocation and Pricing for SDN-enabled Home Networks	2015	Proposes to combine SDN with existing home network infrastructure to enable dynamic control of traffic flows by home users, and guarantee certain QoS using virtualised services. The paper introduces a novel pricing scheme for ISPs, who can perform bandwidth slicing in home networks and implement time-dependent hybrid pricing through SDN APIs. The authors formulate a Stackelberg game to model hybrid pricing/reimbursement strategy for ISPs.	Home network QoE	<ul style="list-style-type: none"> <li>Improving the achievable QoS for the virtualised traffic of home network devices</li> </ul>	Yes	Na	Yes

(Continued)



(Continued)								
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Patro & Banerjee, 2014)	COAP: A Software- Defined Approach for Home WLAN Management through an Open API	2015	Proposes a vendor-neutral cloud-based centralised framework (called COAP) to configure, coordinate and manage heterogeneous and co-located home WiFi APs in dense residential areas (e.g. apartments) using an open API implemented on top of OpenFlow. This paper describes the framework and potential benefits of the framework in home WLANs.	Wireless home network management	<ul style="list-style-type: none"> <li>• WiFi channel configuration</li> <li>• Airtime management</li> <li>• Context-aware AP configuration</li> </ul>	Yes	Implementation of the COAP controller modules over Floodlight controller to communicate with the OpenFlow module at the APs. The authors deployed COAP using OpenWrt based APs across 12 homes for a period of more than 8 months to gather statistics as well as experiment with the basic management capabilities.	Yes
(Sivaraman et al., 2015)	Network-Level Security and Privacy Control for Smart-Home IoT Devices	2015	Proposes a solution for IoT security, which identifies and blocks security/privacy threats at the network level. Three-party architecture is discussed, in which a provider offers security-as-a-service, and an external entity, called the "Security Management Provider" or SMP customizes and delivers to the user extra safeguards at the network level. The authors prototype the idea using SDN platforms, and evaluate its efficacy in protecting multiple smart-home devices.	Smart home/IoT security	<ul style="list-style-type: none"> <li>• Block/quarantine devices, based on their network activity and on the context within the house such as time-of-day or occupancy-level</li> </ul>	Yes	A prototype for the proposed system implementing the three-party architecture and their APIs. The prototype includes enhanced Open vSwitch, FloodLight controller modules for the ISP network, security orchestrator (Ruby on Rails) and web-GUI (JavaScript/HTML) for the SMP.	Yes

(Continued)

<b>(Continued)</b>								
<b>Ref.</b>	<b>Title</b>	<b>Year</b>	<b>Summary</b>	<b>Target application</b>	<b>Example use cases</b>	<b>Cloud based*</b>	<b>Tangible output</b>	<b>OF</b>
(Schulz-Zander, Mayer, Ciobotaru, Schmid, & Feldmann, 2015)	OpenSDWN: Programmatic Control over Home and Enterprise WiFi	2015	Proposes OPENSNDWN, a novel SDN/NFV based WiFi architecture. OPENSNDWN exploits data path programmability to enable service differentiation and fine-grained transmission control, which allows for prioritising critical applications. OPENSNDWN implements per-client virtual access points and per-client virtual middleboxes and supports mobility and seamless migration. OPENSNDWN can also be used to outsource the control over the home network to a third party.	Wireless home network management	<ul style="list-style-type: none"> <li>• Service differentiation</li> <li>• Mobility and migration</li> <li>• Flexible deployment</li> <li>• Flexible control and participatory networking</li> </ul>	Yes**	A prototype implementation for the proposed architecture. The radio interface is implemented in C/C++ while the middlebox Interface is implemented in Python. On the other hand, the controller is based on the Java-based Floodlight OpenFlow controller.	Yes

(Continued)

(Continued)						
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*
(Patro & Banerjee, 2015b)	Outsourcing Coordination and Management of Home Wireless Access Points through an Open API	2015	Similar to (Patro & Banerjee, 2015a), proposes a vendor-neutral cloud-based centralised framework called COAP to configure, coordinate and manage home APs using an open API implemented in the commodity APs. This framework allows the APs to share various types of information with a centralised controller (e.g. interference, traffic, and various flow contexts), and also receive instructions (e.g. configuration and transmission parameters).	Wireless home network management	<ul style="list-style-type: none"> <li>• Better channel assignments via realtime utilisation data from co-located home APs</li> <li>• Managing realtime access of neighbouring APs to reduce contention for important flows (e.g. HTTP based video)</li> <li>• Mitigate hidden terminal interference</li> </ul>	Yes
					An implementation of COAP that extends OpenFlow. The controller modules are implemented over Floodlight to communicate with the OpenFlow module at the APs. The authors deployed COAP using OpenWrt based APs across 12 homes for a period of more than 8 months to gather statistics as well as experiment with the basic management capabilities.	Yes

(Continued)

<b>(Continued)</b>								
<b>Ref.</b>	<b>Title</b>	<b>Year</b>	<b>Summary</b>	<b>Target application</b>	<b>Example use cases</b>	<b>Cloud based*</b>	<b>Tangible output</b>	<b>OF</b>
(Soetens et al., 2015)	SDN-based management of heterogeneous home networks	2015	Evaluates the ability of OpenFlow-enabled switches to manage heterogeneous home networks by utilising redundant links for flow rerouting and perform link switching between wired and wireless technologies both under normal conditions and in case of link failures.	Heterogeneous home networks management	<ul style="list-style-type: none"> <li>Multipath optimisation and resilience</li> <li>Load balancing</li> </ul>	No	An experimental set-up consisting of 4 Linux devices used to simulate a small heterogeneous home environment: a client PC, the home gateway, a network SDN controller and a content server. A simple multipath connection has been established between the PC and home gateway in the form of a wired (Fast Ethernet at 100 Mbps) and wireless (Wi-Fi 802.11g at maximum 24 Mbps) connection. POX is used as an SDN controller. The experimental set-up consists of two Open vSwitch Linux devices located on the client pc and the home gateway.	Yes
(Gharakheili et al., 2015)	Third-Party Customisation of Residential Internet Sharing using SDN	2015	Proposes a system that allows a third party to offer new services through which users can customize Internet sharing within their home networks. The authors develop an over-the-top architecture that enables Internet use customisation, and propose new APIs to facilitate service innovation.	Internet use management	<ul style="list-style-type: none"> <li>Prioritising QoS amongst family members</li> <li>Monitoring Internet usage based on household quota</li> <li>Filtering content based on the age of selected users</li> </ul>	Yes	A fully-functional prototype of the proposed system using SDN. The prototype is deployed in selected households and its usability as well as performance are evaluated to demonstrate feasibility and utility.	Yes

(Continued)

(Continued)						
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*
(Chetty et al., 2015)	uCap: An Internet Data Management Tool For The Home	2015	Presents the design and implementation of a tool (uCap) that runs on home routers and helps home users manage Internet data. Using a cloud-based controller, this tool can provide real-time visibility into and control over network traffic usage in the home. The authors conducted a field trial of uCap in 21 home networks in three countries (South Africa, India, and the United States) and performed an in-depth qualitative study of 10 of these homes. This paper presents the results of the evaluation and implications for the design of future Internet data management tools.	Internet use management	<ul style="list-style-type: none"> <li>• Overview of all household usage</li> <li>• Statistics of data usage and online activities</li> <li>• Control data caps for specific devices</li> </ul>	Yes
					<p>An implementation of the proposed tool, uCap. The interface of the tool is implemented in HTML5 and JavaScript, while the router runs a custom firmware based on OpenWrt (2017), which runs an OpenFlow-enabled software switch that exchanges both traffic statistics and control messages with an SDN controller that is based on Pyretic (Monsanto, Reich, Foster, Rexford, &amp; Walker, 2013).</p>	Yes

(Continued)

(Continued)								
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Nobakht et al., 2016)	A Host-based Intrusion Detection and Mitigation Framework for Smart Home IoT using OpenFlow	2016	Proposes network-based intrusion detection and mitigation framework, called IoT-IDM, to protect smart home environments. IoT-IDM employs SDN to take advantage of its network visibility and programmability. IoT-IDM uses machine-learning techniques to detect compromised hosts. After identifying the source of attacks, IoT-IDM generates appropriate policies and pushes them to underlying routers/switches to mitigate attacks against victim IoT devices.	Smart home/IoT security	<ul style="list-style-type: none"> <li>• Intrusion detection and mitigation</li> </ul>	No	A prototype of the proposed system is developed as a module of Floodlight SDN controller (Project Floodlight, 2017). The five key modules of the prototype are Floodlight application modules. The five modules are: Device Manager, Sensor Element, Feature Extractor, Detection Unit, and Mitigation Unit.	Yes
(Luo et al., 2016)	A Multi-stage Attack Mitigation Mechanism for Software-defined Home Networks	2016	Proposes a multi-stage attack mitigation mechanism for home networks using SDN and NFV. The proposed method relies on performing evidence-driven security assessment first, then selecting an attack mitigation countermeasure for multi-stage attacks.	Home network security	<ul style="list-style-type: none"> <li>• Mitigating multi-stage attacks</li> </ul>	No	A case study to evaluate the proposed scheme.	No

(Continued)

(Continued)						
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*
(Abuteir et al., 2016)	An SDN Approach to Adaptive Video Streaming in Wireless Home Networks	2016	Introduces a new technique to enhance the QoE of video streaming at the gateway without modifying the client or the video server. The proposed technique is realised as a framework that runs on top of SDN controllers and performs dynamic traffic shaping based on collected network traffic statistics, allocating bandwidth for the clients in real time. The framework is evaluated against fairness, instability, average video quality and video traffic utilisation.	Home network QoE	<ul style="list-style-type: none"> <li>Fair sharing of a wireless medium among home users by allocating them bandwidth proportionally to their links qualities</li> </ul>	No
					An implementation of the proposed framework in NS3 simulator (ns-3, 2017). The authors implemented a new module for NS3 to simulate the DASH video streaming and encoded an open source film using FFmpeg (2017) stream over the network.	Na

(Continued)

(Continued)								
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Yang et al., 2016)	Conan: Content-aware Access Network Flow Scheduling to Improve QoE of Home Users	2016	Introduces an architecture that enables content-aware flow scheduling in access networks to improve home user QoE. SDN is used to provide flexible bandwidth allocation of downstream traffic. Automatic identification of specified applications is deployed at each home gateway instead of the centralised SDN controller. The service requests of identified flows are forwarded to the controller and the corresponding rules to serve those flows are installed in the data plane.	Home network QoE	<ul style="list-style-type: none"> <li>Bandwidth allocation for HTTP video streaming</li> </ul>	Yes	An evaluation of the proposed architecture to measure the performance on video streaming. To perform the experiments, two components are implemented: the broker that is deployed at the home gateway, and the centralised controller that receives requests and assigns network resource for downstream traffic.	Na
(Bozkurt & Benson, 2016)	Contextual Router: Advancing Experience Oriented Networking to the Home	2016	Presents Contextual Router, a management framework for home networks that incorporates user preferences, the context of user interactions and application models in determining resource allocations for optimal network utility. Contextual Router is aimed to improve page load times and reduce buffering events and buffering time.	Home network QoE	<ul style="list-style-type: none"> <li>Monitor individual flows and capture user contexts</li> <li>Enforce bandwidth allocations for individual applications</li> </ul>	No	A prototype implementation in which the contextual monitors are developed as OS daemons that send reports to the home gateway, then the controller. Contextual routers are built atop BISMart routers, where each router is an OpenWrt router that runs Open vSwitch. The contextual controller is an SDN application on Floodlight.	Yes

(Continued)



(Continued)								
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Jang et al., 2016)	Design A Bandwidth Allocation Framework for SDN Based Smart Home	2016	Proposes a bandwidth allocation framework for IoT enabled smart homes, where an ISP is assumed to support thousands of smart homes, and each home is equipped with tens of IoT devices. The proposed framework uses SDN to optimize bandwidth allocation on internal home traffic and external Internet traffic.	Home network QoE	<ul style="list-style-type: none"> <li>Optimize bandwidth allocation</li> </ul>	Yes	Na	Yes
(Gallo et al., 2016)	SDN@home: A Method for Controlling Future Wireless Home Networks	2016	Presents a software-defined multi-technology network architecture (SDN@home) and demonstrates how a future home gateway (SDN controller) can directly and dynamically program network devices. The proposed SDN@home architecture defines a new type of flexibility where wireless protocols and features are no longer tied to specific technologies but can be used by general-purpose wireless SDN devices.	Wireless home network management	<ul style="list-style-type: none"> <li>Flow-level device control, where the controller is mainly responsible for diverting traffic flows across the technologies in each device</li> <li>Link-level device control, where the controller is also responsible for configuring the behaviour of the links</li> </ul>	No	Na	Na

(Continued)

(Continued)								
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Xu et al., 2016)	Toward Software Defined Smart Home	2016	Proposes software defined smart home platform, SDSL, based on the idea of SDN. The proposed platform exploits the design features of virtualisation, openness, and centralisation to integrate the heterogeneous network devices in smart home environments, and adapt to the great difference between user demands. This article also discusses the application value of the proposed platform and its underpinning technologies.	Smart home/IoT management	<ul style="list-style-type: none"> <li>Home automation services based on user location</li> <li>Configurable lifestyle management</li> <li>Condition monitoring and automatic home services</li> </ul>	Yes**	Na	Na
(Bakhshi & Ghita, 2016)	User-Centric Traffic Optimisation in Residential Software Defined Networks	2016	Proposes a dynamic queuing-based user-centric traffic optimisation scheme utilising user traffic profiles and user defined profile priorities to effectively manage the allocated bandwidth among several users in a residential SDN. This paper also proposes an SDN traffic monitoring and management application for implementing Linux-based hierarchical token bucket (HTB) queues customised for individual user profiles in real-time, according to user-defined priorities.	Home network QoE	<ul style="list-style-type: none"> <li>Utilising user-defined profile priorities for bandwidth allocation</li> </ul>	No	An evaluation of the proposed design on test profiles using Mininet. Traffic is generated in software, and the network consists of 10-18 user machines and 5-10 web servers added at different stages to observe variation in traffic statistics, two switches for home-gateways and an ISP router. This design employs the Ryu controller supporting OpenFlow.	Yes

(Continued)

<b>(Continued)</b>								
<b>Ref.</b>	<b>Title</b>	<b>Year</b>	<b>Summary</b>	<b>Target application</b>	<b>Example use cases</b>	<b>Cloud based*</b>	<b>Tangible output</b>	<b>OF</b>
(Taylor et al., 2016)	Whole Home Proxies: Bringing Enterprise-Grade Security to Residential Networks	2016	Explores combining SDN and proxies with commodity residential Internet routers. The authors propose and evaluate a "whole home" proxy solution for the Skype video conferencing application to test the feasibility of the idea in practice. The proposed approach can automatically detect when a device is starting to use Skype and dynamically intercept all of the Skype traffic and route it through a proxy without disturbing unrelated network flows.	Home network security	<ul style="list-style-type: none"> <li>Setting a proxy for certain applications such as Skype</li> </ul>	Yes	An implementation of the proposed approach using a consumer-grade router that sends flows to a remote OpenFlow controller on a server in a cloud data centre. A TP-LINK TL-WR1043ND router is flashed with a custom build of the OpenWrt image, and the kernel-level Open vSwitch package is selected.	Yes

(Continued)

(Continued)						
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*
(Flores Moyano, Fernández, Bellido, & González, 2017)	A software-defined networking approach to improve service provision in residential networks	2017	Proposes to improve the provision of new services and to increase the usability of residential networks by upgrading the residential gateway based on SDN and NFV. In the proposed approach, SDN provides a fine-grained control of the traffic and NFV outsources traditional and specialised network functions running inside the RGW like routing or network address translation to the ISP. A management framework is designed based on the proposed approach, where the residential user is involved in the management tasks through the provision of network management applications and network applications are decoupled from the underlying SDN controller technology to encourage the development of innovative network applications.	Home network management	<ul style="list-style-type: none"> <li>• Network Access Control</li> <li>• Parental control</li> <li>• Device accounting</li> <li>• Traffic meter</li> </ul>	Yes
					<p>A POC for the proposed approach. The experimental scenario is created using a virtualised testbed containing virtual machines. Each VM emulates a VMANDO, a vCSD, or a user device. To evaluate the controller-agnostic approach, two different controllers are used: Floodlight and Pyretic. The SDN application layer is developed in Python, while the adaptation and network application levels are coded as controller modules. The GUI is developed using the Django framework, and PostgreSQL is used to store information about network configuration and permissions.</p>	Yes

(Continued)

(Continued)							
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	
(Moyano et al., 2017)	A user-centric SDN management architecture for NFV-based residential networks	2017	Proposes a new user-centric management architecture to engage home network users in the management tasks of their own networks, improving the usability and enabling the provision of new services. In this approach, residential network management applications are split into two components: a front-end for user interaction, running on the user preferred device (PC, laptop, smartphone); and a back-end built on top of SDN and NFV paradigms. The solution takes advantage of the fine-grained control of network traffic and the convenience to communicate network events provided by SDN and the outsourcing of traditional network functions like routing or NAT from the residential gateway to a cloud-based ISP infrastructure.	Home network management	<ul style="list-style-type: none"> <li>Parental Control app</li> <li>Network Status app</li> <li>Switching</li> <li>Device Tracking</li> </ul>	Yes	
						<p>A POC for the proposed approach, which is created in a virtualised testbed to emulate a real scenario composed by the ISP cloud infrastructure, the residential networks and the access network.</p> <p>The Control and SDN Application layers are implemented using Floodlight, of which some modules are modified. The Management layer is developed in Python. At the Interaction layer, the corresponding clients are implemented as Android apps.</p>	Yes

(Continued)

(Continued)								
Ref.	Title	Year	Summary	Target application	Example use cases	Cloud based*	Tangible output	OF
(Stewart et al., 2017)	CommunityGuard: A Crowdsourced Home Cyber-Security System	2017	Introduces the design, prototype, and evaluation of CommunityGuard, an in-line home cyber-security system where a Guardian Node in each home shares new threats with nodes in other homes. This provides a sort of herd immunity against new attacks. As soon as an attack claims a victim, the victim's peers will be informed, and will repel the same attack against their own subnets. Furthermore, Guardian Nodes regularly update themselves with latest threat models to provide effective security against new and emerging threats.	Home network security	<ul style="list-style-type: none"> <li>Defeating DDoS attacks by stopping the traffic at the weaker end of its path, which is the source subnet (home network)</li> </ul>	Yes	Initial prototype of the proposed system, in which the Guardian Node is implemented as a BeagleBone Black device (BeagleBoard, 2017), and is capable of having network functions deployed onto it and remotely configured, while the Community Outpost is deployed as the Snort intrusion prevention system (Cisco, 2017).	Na
(Moyano et al., 2017)	NFV-based QoS provision for Software Defined Optical Access and Residential Networks	2017	Extends the scope of SDN technologies to optical access networks and brings cloud technologies to the edge of the network in order to enable the creation of advanced residential networks and provide traffic differentiation.	Home network QoE	<ul style="list-style-type: none"> <li>Traffic differentiation</li> </ul>	Yes	An initial experimental testbed to validate the proposed solution is still being developed and described. The focus of the testbed is on the Software Defined Optical Access Network (SDOAN) component.	Yes

(Continued)

<b>(Continued)</b>								
<b>Ref.</b>	<b>Title</b>	<b>Year</b>	<b>Summary</b>	<b>Target application</b>	<b>Example use cases</b>	<b>Cloud based*</b>	<b>Tangible output</b>	<b>OF</b>
(Hernando et al., 2017)	Virtualisation of Residential IoT Functionality by Using NFV and SDN	2017	Proposes to leverage the virtualisation capabilities of NFV and the programmability of SDN to offer a portfolio of IoT-related functions to home users. The aim is to reach economies of scale by offering inexpensive customer premises equipment supporting most IoT physical communication options, while vendor-specific functionality is externalised and implemented by the ISP or third parties.	Smart home/IoT management	<ul style="list-style-type: none"> <li>Recognize and manage IoT hardware belonging to different manufacturers</li> <li>Security updates of IoT devices</li> </ul>	Yes	Na	Na

\*relies on a ISP/third-party controller

\*\* optional



© 2018 The Author(s). This open access article is distributed under a Creative Commons Attribution (CC-BY) 4.0 license.

You are free to:

Share — copy and redistribute the material in any medium or format.

Adapt — remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made.

You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

No additional restrictions

You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

***Cogent Engineering* (ISSN: 2331-1916) is published by Cogent OA, part of Taylor & Francis Group.**

**Publishing with Cogent OA ensures:**

- Immediate, universal access to your article on publication
- High visibility and discoverability via the Cogent OA website as well as Taylor & Francis Online
- Download and citation statistics for your article
- Rapid online publication
- Input from, and dialog with, expert editors and editorial boards
- Retention of full copyright of your article
- Guaranteed legacy preservation of your article
- Discounts and waivers for authors in developing regions

**Submit your manuscript to a Cogent OA journal at [www.CogentOA.com](http://www.CogentOA.com)**

