# The *Majord'Home*: a SDN Approach to Let ISPs Manage and Extend Their Customers' Home Networks

Mathieu Boussard, Dinh Thai Bui, Richard Douville, Nicolas Le Sauze,
Ludovic Noirie, Pierre Peloso, Rémi Varloot, Martin Vigoureux
Alcatel-Lucent Bell Labs France
Centre de Villarceaux, Route de Villejust,
91620 Nozay, France
Email: first.last@alcatel-lucent.com

***Abstract*—As the number and variety of connected devices increase, most end-users find themselves unable to manage their home networks properly, not having enough time and/or knowledge to do so. In this paper, we propose a new approach to remove this burden from them, by fully virtualizing the home network and delegating its management and operations to the ISP, while keeping end-users in control. We furthermore define the architecture of our software-based *Majord'Home* solution. Acting as a majordomo of the home, it handles a representation of the home objects and network constraints, automates the connectivity between heterogeneous elements and thus meets the needs of end-users. We finally describe the first version of our on-going implementation as a proof of concept.**

## I. Introduction

The advent of the Internet of Things (IoT) in our homes imposes to cope with a larger number of heterogeneous connected devices. However, configuring the home networks is already a painful task for end-users, which may in turn slow down the development of future smart homes.

Inspired by some previous works (e.g., [1], [2], [3]), this paper proposes a new software-based approach to delegate the control and the management of home networks to Internet Service Providers (ISPs) by virtualizing the connected devices.

This paper is organized as follows. In section II, we explain the needs for virtualized and ISP-managed home networks. We then introduce in section III the concept of *Communities of Connected Objects* that helps the operator in the management of home networks. We develop in section IV the architecture of the *Majord'Home* in charge of this automated management. Finally, we describe in section V the ongoing implementation of this architecture in a multi-home demonstrator.

## II. Virtualized and ISP-managed home networks

In this section, we first describe the burden of home network management by end-users, then we propose and defend a solution that delegates this task to the ISP using virtualization.

### *A. Increasing complexity of home network management*

Historically, home networks comprised few elements so their management was not an issue. The number of connected devices surrounding us is however constantly increasing in what is known as the IoT, especially at home with the emergence of connected TVs, set-top boxes, tablets, phones, network-attached storage and many other smart objects or appliances embedding a network interface.

End-users are the operators of their home networks and consume a lot of applications and services. As such, they painstakingly experience the complexity of configuring and operating those networked devices, as well as the frustration of not being able to live the rich experiences that the seamless combination of their capabilities should procure them [1].

Furthermore, this complexity impacts the ISPs whose hotlines are saturated by customers' complaints about malfunctions or bad quality of experience, while most problems arise from misconfigurations or lack of knowledge from end-users.

**Our solution:** *To remove the burden of home network management from end-users, we propose to have the ISP manage its customers' home networks by virtualizing connected objects and network elements. The end-users keep control through a simplified interface, on which they express their expectations that are translated into low level configuration instructions, under a Sofware-Defined Network (SDN) framework.*

In the following, we explain the rationales for delegating the home network management to the ISP and for virtualization.

### *B. ISP-managed home networks*

Offloading the configuration tasks from end-users implies delegating them to another entity. It could be:

1) the ISP, that already has trusted customer management services and controls the network connecting homes;
2) an Over-The-Top (OTT) service provider, deploying a box or software in the homes and a service in overlay of the network and relying on a *cloud* infrastructure.

Following option 1, our solution allows the full integration of smart home and network services, while some ISPs propose only partial solutions today, either by providing evolved home gateways (e.g., *Freebox*[1] by Free or *Livebox*[2] by Orange), or very specific smart home services (e.g., Verizon *Home Control*[3] or Orange *Smart Home*[4]). On the contrary, authors of [2] propose a solution similar to option 2.

[1] http://en.wikipedia.org/wiki/Freebox
[2] http://en.wikipedia.org/wiki/Orange_Livebox
[3] https://www.verizon.com/homecontrol
[4] http://hello.orange.com/plus-loin-avec-les-nouveaux-usages/smart-home

Whatever the chosen option, the following key requirements should be met ([1], [2]):

- *Home view*. The solution must have an accurate view on the devices within the home network and thus be close enough in order to effectively control and manage it.
- *Home privacy and security*. The users must keep control on the access to their devices and their data. The solution should implement access control and traffic isolation, while preserving the privacy about personal data usage.
- *User-friendlessness*. The users should not have technical knowledge but just use an friendly service interface.
- *Extended Home and QoS*. The solution should provide to end-users some extended home capabilities such as remote access to home devices and services while in mobility or on-demand interconnection with their friends' homes using short-lived service-centric overlay networks for some devices. Doing so, one must ensure the Quality of Service (QoS) required for the different usages: low latency, sufficient bandwidth, service availability, etc.
- *Openness*. In order to facilitate the future evolution of home networks, the solution must handle heterogeneous connected devices and any service using them. Thus the solution must offer open interfaces to third parties.

For most of these requirements, options 1 and 2 have similar characteristics such as being close to the home networks and managing many of them, which gives them similar advantages. An exception is the *extended home and QoS* that requires to have the right view on both the ISP network and the home network. Our option is better positioned for this as it is tightly linked to the know-how and assets of the ISP.

### C. Towards virtualized home networks: an SDN approach

We propose to remove the home network configuration and management tasks from end-users, so the data and control planes should be decoupled like in SDN [4].

Independently of the owning actor, it is reasonable to assume that the entity controlling and managing the home network relies on *virtualization* techniques to have its own representation of the connected objects within the home network and manipulate them in order to render the right services.

Virtualization in home networks has already been proposed, for example in [3]. As argued in other network segments with SDN, it decreases the complexity of management and facilitates the deployment of new services in the networks.

## III. Communities of Connected Objects

In this section, we define the concept of Communities of Connected Objects (CoCO), as well as some other associated concepts. The CoCO concept is one of the pillar of the overall architecture defined in section IV.

### A. Connected Objects and Virtual Objects

**Definition—Connected Object (CO):** *A connected object is an entity with which one can interact through the network.*

It can be anything: the nature of the CO is intentionally broad: a physical object, an application, a software, etc.

**Definition—Virtual Objects (VO):** *A virtual object is an abstract representation of a CO, part of a CO, or of an entity distributed over multiple COs.*

VOs specify certain characteristics of the COs, such as a list of compatible protocols, the connected object availability, etc. The primary motivation behind VOs is the need for a homogeneous representation of COs, like in SDN [4].

A second feature of VOs is that they could serve as a proxy. The VO may provide additional means (e.g. additional standard protocols) to interact with the CO even if the underlying connected object(s) only recognizes a device specific protocol.

VOs can be divided into two categories: virtual devices, which consist in one-to-one representations of physical connected devices, and virtual services, which aggregate, specialize or otherwise refine other virtual objects.

### B. Communities of Connected Objects

**Definition—Community of Connected Objects (CoCO):** *A community of connected objects is a set of VOs which have agreed to interconnect for some specific purpose.*

VOs in a CoCO are interconnected via a SDN-controlled Virtual Network (VN). Within this VN, broadcast and multicast messages should particularly be handled as per the support of discovery protocols such as UPnP[5].

A CoCO must be managed at multiple levels:

- what protocols can be used;
- possible services provided by the CoCO itself, which may require processes running somewhere within the network;
- the network level, which must ensure the connectivity between the VOs in the CoCO (VN).

### C. Avatars

**Definition—Avatar:** *An avatar is the representation of a user, mainly to manage the rights of this user over its VOs.*

The avatar is especially important during the creation of a CoCO, where including VOs requires some authentication to prove that the user is legitimate in doing so. Alternatively, the avatar can be thought of as a user's "login" when managing his virtual objects through an interface. In some cases, avatars may also be able to act on behalf of the user.

## IV. Architecture of Majord'Home

In this section, we describe our software-based solution to manage the home networks and its functional architecture.

### A. Majord'Home: the majordomo of the home network

**Definition—Majord'Home:** *Similarly to what happens in wealthy households, the ISP plays the role of the majordomo of its customers' home networks. We call Majord'Home the software that controls and manages the home networks.*

There is logically one *Majord'Home* per home, as that is its natural scope and isolation between homes for security and privacy requirements should be enforced.

[5] http://upnp.org/

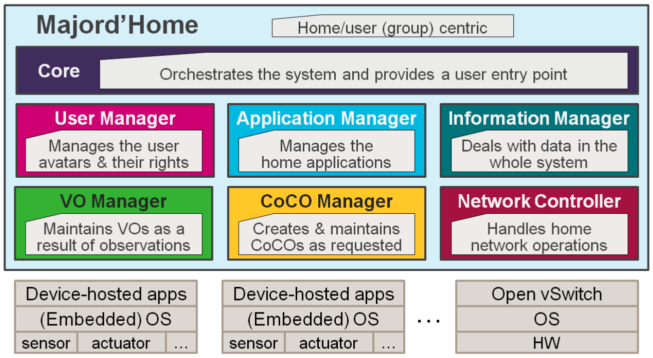
Majord'Home
Home/user (group) centric
Core
Orchestrates the system and provides a user entry point
User Manager
Manages the user avatars & their rights
Application Manager
Manages the home applications
Information Manager
Deals with data in the whole system
VO Manager
Maintains VOs as a result of observations
CoCO Manager
Creates & maintains CoCOs as requested
Network Controller
Handles home network operations
Device-hosted apps
(Embedded) OS
sensor
actuator
…
Device-hosted apps
(Embedded) OS
sensor
actuator
…
…
Open vSwitch
OS
HW

Figure 1. Architecture of the Majord'Home

Each *Majord'Home* has the full view on the COs belonging to its home. It interacts with other *Majord'Homes* when services require devices belonging to other homes. They manages VOs, CoCOs and avatars defined in section III.

End-users keep control by interacting with their *Majord'Home* with a user-friendly interface. The *Majord'Home* is aware of end-users and has a view on the services and their relevant devices in the home network.

## B. Functional building blocks of the Majord'Home

Figure 1 represents the different functional building blocks of the *Majord'Home* architecture.

The ***core*** of the *Majord'Home* is in charge of orchestrating all the other functional building blocks. It is the entry point of the *Majord'Home* system and has an IP address in order to be contacted when required. It is connected to:

- applications embedded in the connected devices;
- home network nodes (e.g., residential gateway, router, switch), using the Network Controller described below;
- *Majord'Homes* of other home networks;
- more generally, the ISP network and the Internet.

The ***User manager*** handles the users' avatars with their access rights in the home networks.

The ***VO manager*** maintains the VOs for COs within the home, responding to events from the network manager (e.g., new COs).

The ***CoCO manager*** dynamically handles the CoCOs by creating them upon request from a user or an application. It maintains their state by keeping trace of the state of VOs that compose them and terminates them when needed.

The ***Application manager*** allows to deploy new applications within the smart home context and rely on VOs or CoCOs. These applications can be offered by the ISP owning the *Majord'Home* or by third party service providers.

The ***Network controller*** handles the home network configuration operations, as well as communication within the home network and with the outside (Internet or other home networks). It ensures the traditional network features of the home gateway (e.g., NAT, open/close ports, QoS tagging, etc).

The ***Information manager*** handles in some repositories the information about COs, VOs, CoCOs, users' avatars, used applications or services and network capabilities, which is used by the other functional blocks.

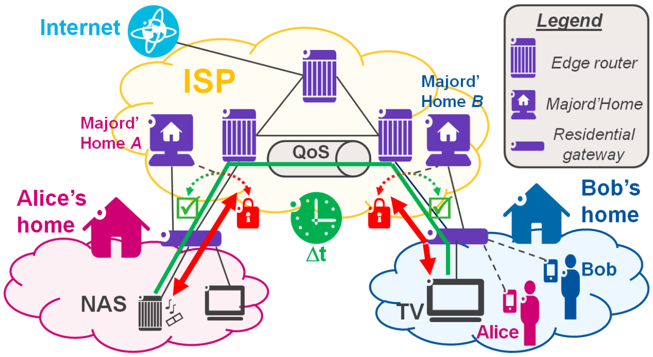

Figure 2. Scenario of the demo

## V. First demonstrator

To consolidate our proposal and validate its feasibility, we describe in this section the ongoing implementation of the first version of the *Majord'Home* prototype that applies the architecture of section IV in a multi-home scenario.

## A. Scenario

The scenario is about the interconnection of two private COs located at two different home networks that are seamlessly used together thanks to our solution. The scenario is described in figure 2. We consider Alice and Bob's home networks, both of which contain several COs. The different steps of our demo scenario are:

1) Alice is in Bob's home where she has Internet access. She wants to use Bob's (private) TV to watch a video stored in her (private) media server (Network-Attached Storage, NAS) located at her home.
2) She sends a service request to her *Majord'Home A*, asking it to perform the operation for her.
3) *Majord'Home A* contact Bob's *Majord'Home B* that sends a request to Bob to authorize the interconnection.
4) *Majord'Homes A* and *B* jointly set the CoCO to allow the private devices to communicate for a limited lifetime $\Delta t$ (either explicit or implicit, e.g., time-out).
5) Alice uses Bob's TV to watch the video from her media server as if both devices were located within the same LAN (e.g., using standard UPnP discovery procedures).
6) Upon expiration of the lifetime $\Delta t$, the CoCO instance and the communications means are removed.

While the scenario looks fairly similar to features available with existing devices, it actually comprises strong differences:

- When Alice is connected at Bob's home, she only has a visibility on devices that Bob allowed to share (the TV here) and not to all Bob's home devices.
- Communication paths between VOs amongst a CoCO are established on-demand thanks to the SDN framework, offering total isolation between disjoint CoCOs. This offers more security and privacy than legacy home networks.
- While the remote connection of Alice to her home follows a normal (Best Effort) route in the core network, the media session flow can be tagged to follow a QoS-guaranteed route in this network.

### B. Majord'Home implementation

The whole of the *Majord'Home* is implemented within the Open Services Gateway initiative (OSGi) framework for modularity, along with Jetty[6] and Jersey[7] to expose the various components (VOs, Users, CoCOs, Applications) and their managers through a set of REST[8] APIs.

The ***Core*** is on top of other blocks. It relies on a notification engine used both for internal orchestration and for dynamic states synchronization with the various clients and remote *Majord'Homes*.

Each of the following managers relies on the generalization of an architecture formerly designed within an anterior work around our virtual object gateway [5], significantly extended with various dimensions, like handling of user access control and customization of the provided content.

The ***User manager*** currently uses the Apache Shiro[9] Java security framework to perform the authentication, authorization and session management used over all the components of the Majord'Home. It additionally performs the administration of users and their permissions.

The ***VO manager*** has slightly evolved since the original VO framework [5]. Still providing an interface to present and manipulate the VOs, it now allows the dynamic instantiation of new VOs according to detection of new COs in the Home Network. The VOs themselves have been empowered with network abilities that allows them to be identified and to join different communities.

The ***CoCO manager*** is a specific addition that allows to create, manipulate and present CoCOs. An inference engine (like FactPlusPlus[10] or Hibernate[11]) is used to suggest the creation of CoCOs according to the semantic descriptions (e.g., OWL[12]-based) of the VOs and their capacities.

The ***Application manager*** is not required in this first demonstrator because our use-case relies on native UPnP/DLNA embedded in the COs.

The ***Network controller*** relies on SDN/Openflow[13] to pilot Open Virtual Switches (OVS, Open vSwitch[14]). It is made of two essential components. The first one interfaces with other components of the *Majord'Home* in order to acquire the information on CoCOs and the associated VOs. The second one is an SDN-controller that allows for implementing the network connectivity according to the network policies required by a given CoCO. It is built upon the open-source SDN-controller *Open DayLight*[15]. Its main role is to translate CoCO policies into OVS rules and to classify those rules into different OVS tables in order to reach a scalable implementation.

### C. Demo set-up

The ISP network is emulated by three Alcatel-Lucent 7750 Service Routers forming an Autonomous System interconnected to the Internet and providing on-demand assured-quality connectivity services [6]. In our scenario, a connectivity with bandwidth constraints between Alice and Bob homes is triggered at the creation of the CoCO to conform with the expected quality of experience for high quality video delivery.

Alice and Bob's home networks have many COs. The NAS in Alice's home is a PC with DLNA server capability. A connected TV in Bob's home has a DLNA renderer capability. Each home network is connected to a router of the ISP network with a server playing the role of the home gateway. More precisely, the home gateways are virtualized and, like the *Majord'Homes* and the OVS, their functions such as Firewall, NAT and DHCP have been deployed on some servers.

Finally the demo set-up contains two mobile devices running a *Majord'Home* client which is an Android application implemented for the demo, one is used by Bob (configured with its credentials), the other is used by Alice. They are connected to Bob's home network by WiFi.

## VI. Conclusion

We proposed a new solution to help the ISPs manage their customers' home networks: the *Majord'Home*. Virtualizing the home network with the concepts of VOs, Avatars and CoCOs, we defined a preliminary software architecture. To validate the feasibility, we are implementing a first prototype that we are applying on an extended-home scenario.

This *Majord'Home* concept requires future research works in many directions: extension to various use-cases to test and illustrate the strength of our approach, consolidation of the architecture with SDN [4], introduction of autonomic and cognitive concepts to help having a smart and autonomous solution, broadening of the scope to smart cities, etc.

## Acknowledgment

The authors thank their colleagues Benoît Christophe, François Dorgeuille, Benoît Ronot and Dominique Verchère for their involvement in the demo, as well as Laurent Ciavaglia and Michel Le Pallec for discussions about the concept.

## References

[1] W. K. Edwards, R. E. Grinter, R. Mahajan, and D. Wetherall, “Advancing the state of home networking,” *Commun. ACM*, vol. 54, no. 6, pp. 62–71, Jun. 2011.

[2] R. Brennan, Z. Etizoni, K. Feeney, D. O'Sullivan, W. Fitzgerald, and S. Foley, “Consumer-managed federated homes,” *Communications Magazine, IEEE*, vol. 52, no. 6, pp. 194–201, June 2014.

[3] T. Cruz, P. Simoẽs, N. Reis, E. Monteiro, F. Bastos, and A. Laranjeira, “An architecture for virtualized home gateways,” in *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on*, May 2013, pp. 520–526.

[4] Open Networking Foundation (ONF), “SDN architecture, Issue 1,” https://www.opennetworking.org/, Technical Paper, June 2014.

[5] M. Boussard, B. Christophe, O. Le Berre, and V. Toubiana, “Providing user support in web-of-things enabled smart spaces,” in *Proceedings of the Second International Workshop on Web of Things*, ser. WoT '11. New York, NY, USA: ACM, 2011, pp. 11:1–11:6.

[6] FP7 ETICS consortium, “Economics and Technologies for Intercarrier Services,” https://www.ict-etics.eu/, Final white paper, 2013.

[6] http://www.eclipse.org/jetty/

[7] https://jersey.java.net/

[8] http://en.wikipedia.org/wiki/Representational_state_transfer

[9] http://shiro.apache.org/

[10] https://code.google.com/p/factplusplus/

[11] http://hibernate.org/

[12] http://www.w3.org/2004/OWL/

[13] https://www.opennetworking.org/

[14] http://openvswitch.org/

[15] http://www.opendaylight.org/