Collaborative Cloud-based Management of Home Networks

Bilhanan Silverajan, Juha-Pekka Luoma, Markku Vajaranta, Riku Itäpuro
Tampere University of Technology, Finland
Email: firstname.lastname@tut.fi

***Abstract*—Future home networks are expected to become extremely sophisticated, yet only the most technically adept persons are equipped with skills to manage them. In this paper, we provide a novel solution as to how complex smart home networks can be collaboratively managed with the assistance of operators and third party experts. Our solution rests in separating the management and control functionalities of the home access points and routers, away from the actual connectivity, traffic forwarding and routing operations within the home network. By so doing, we present a novel REST-based architecture in which the management of the home network can be hosted in an entirely separate, external cloud-based infrastructure, which models the network within the home as a resource graph.**

***Index Terms*—Homenet, Network Management, Cloud, IoT.**

I. Introduction

Many residential home networks today consist of little more than a broadband-enabled WiFi access point and Network Address Translator (NAT), offering wireless and wired connectivity to any and all authenticated end-devices. If wireless coverage is spotty, wireless repeaters are used to cover blind spots. If application network performance is deemed to be laggy, more bandwidth is acquired from an Internet Service Provider (ISP). Granting connectivity to new devices or providing visitor access is typically accomplished by sharing a well-known password for wireless access. Therefore, apart from occasional activity, present practices require minimal management of the residential wireless home network by the home owner.

In recent years however, the home has rapidly become a natural convergence point for emerging technological developments and innovations. The smart home of tomorrow is expected to be an integral industrial and commercial testbed for the Internet of Things (IoT), Smart Cities and Grids, and even 5G connectivity. Connected homes are rapidly becoming a fertile ground for commercial vendors introducing their own ecosystems for home automation, health care and remote monitoring. This is widely anticipated to produce a rapid proliferation of computing, sensing and actuation systems in the home. Many of these systems also are integrated with home owners' personal mobile devices and into cloud-based platforms. At the same time, traditional Internet usage and connectivity usage scenarios would continue to play an important role.

Needless to say, these developments present severe strains onto any residential home network. To allow large numbers of sensors and smart devices to be connected and reachable via the Internet, network addresses need to be efficiently and properly allocated. Various members of a family may have different needs and connectivity priorities for their connected devices, while device vendors, utility and electricity providers may equip a smart home with their own products which may or may not be connected to the provider's network via the home network. A home network owner may also wish to segregate visitor network traffic away from critical portions of the network itself, giving rise to the need to perform network segmentation, traffic shaping and routing. Management of such a residential home network poses a few problems. Firstly, it is highly challenging for an average home owner to administer complex networks. Secondly, any technical assistance sought currently for management of access points and servers in the home relies upon the ability to remotely or physically access the customer premise equipment (CPE) which may not always be possible, owing to geographical issues or the presence of dynamic IP addresses, NATs as well as firewalls if other network routers or access points are positioned arbitrarily within the home network topology.

In this short paper, we address this challenge, as to how operators and third party experts can assist home owners in managing complex networks of the connected home in the future. Our focus is specifically on residential home networks that comply with the IETF Homenet standards and architecture. A brief description of Homenet is provided in Section II. We provide a novel solution of managing the home network in an external cloud using a browser based GUI or a REST-based interface, that integrates well with other REST-based and IoT services for added value to the home owner. The design and implementation of our solution are elaborated upon in Sections III and IV. With proper access control and authorisation methods in place, this provides a far more flexible and convenient solution for co-managed networks to be viewed by external parties, without having to manage individual home routers using traditional methods requiring remote access and local login credentials for each router. This is discussed in Section V. We then conclude this short paper in Section VI.

II. IETF Homenet

The Home Networking (Homenet) Working Group was chartered in 2011 by the Internet Engineering Task Force (IETF), in anticipation of the growing complexities of residential home networks, with the increase in number and

demands by both connected computing devices and IoT-type constrained nodes. Homenet's intent is to research and standardise networking protocols and other mechanisms useful for residential home networks [1]. Although the properties and network topologies in a home network are not mandated, the home network is envisioned to grow large enough to require multiple network segments and subnets within the home, implying the existence of several routers which need to be orchestrated to perform actual routing using one more more well-known interior gateway routing protocols such as Babel [2], OSPF [3] or RIP [4]. Homenet supports both IPv6 and IPv4 address allocation mechanisms. Additionally Homenet advocates each node in the network to possess both a globally unique IPv6 address, as well as a local IPv6 address to avoid operational communications disruptions within the home, should an ISP uplink incur any downtime. Multiple ISP uplinks can be present in a Homenet-based network. Finally, a Homenet Control Protocol (HNCP) [5] is being specified, with which participating routers obtain information about the network capabilities, routing protocols and services present in the home network.

III. Design

Our approach has been inspired partly by Software Defined Networking (SDN) based principles, in which the network management and configuration functions of the home are reflected in the cloud and separated from the traffic flow and routing aspects of the home network. While common practices in SDN-based networks aim at real-time control of network elements, we choose to apply SDN concepts for network configuration management. Hence, direct control of packet flows and protocols such as OpenFlow are outside our scope. This is reflected in our architecture, as shown in Figure 1.

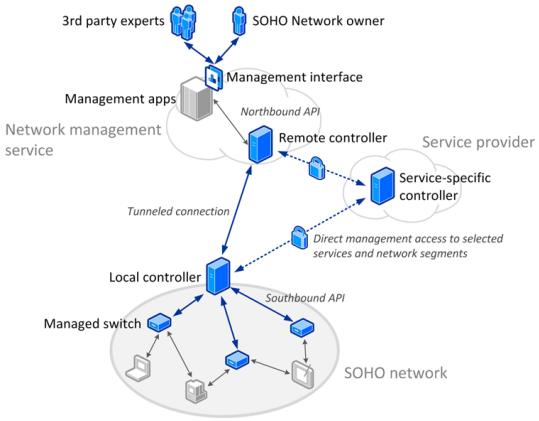

Figure 1: Proposed architecture

A cloud-based platform (henceforth referred to simply as a 'cloud') serves as a centralised network management and control platform to remotely manage home networks. This effectively behaves as a remote SDN controller, while having the network management service in the cloud provides a platform for the development and use for various kinds of operator tools, services and new network management apps, both native and web-based. The cloud interfaces with a trusted device that acts as a local controller, instead of directly communicating with the home network equipment. While the cloud provides a management interface and an effective means to deliver decisions to the home network, a local controller, possessed by the home owner, serves as a control point to execute decisions taken by the cloud-based controller, into the home network. To act as a local controller, a trusted device such as the owner's smartphone needs access to the Internet-based cloud service hosting the remote controller, and either a direct or tunnelled access to the home network. These connections need not be available at the same time if caching of configuration data is used by the smartphone.

If network configuration changes are made in the cloud, the smartphone can be made aware of any updates to the homenet configuration. Should the cloud provide a push-based notification service, the notification triggers management actions by the smartphone on the native management interfaces of homenet devices. If push notifications are not supported, REST-based polling by the smartphone can be used instead. Finally, the smartphone then connects to each element in the home network automatically to deliver the changed configuration. This is illustrated in Figure 2, and further elaborated upon in Section IV.

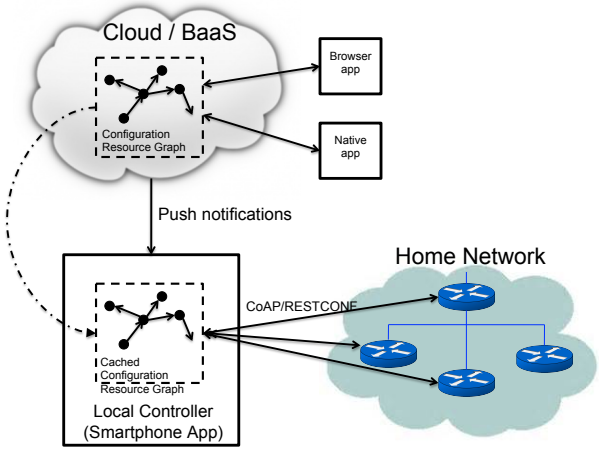

Figure 2: Collaborative Management Design

IV. Implementation

Our test environment for prototyping our cloud-based collaborative network management solution consists of several portions. Firstly, we created an ISP capable of providing Internet connectivity to various home networks via IPv4 and IPv6. A DHCP server delivers a single IPv4 address to home border routers (as most ISPs do today), while IPv6 prefix delegation consisting of a /60 prefix is provided to supply the home network with global IPv6 addresses. Secondly, we then deployed a Homenet-compliant residential network with four wireless access points (consisting of TP-Link TL-WDR4300 and Buffalo WZR-HP-AG300H). The stock firmware was replaced with the latest OpenWRT snapshots from the trunk,

based on Linux kernel version 3.10.49. The 2.4 GHz radio interfaces provided WiFi connectivity to client devices in the home, while all the 5 GHz radio interfaces were dedicated towards creating a wireless mesh network, in which the Babel routing protocol was utilised. This allowed for a resilient residential network where the network topology adjusted to favour routes with the strongest link characteristics, while remaining transparent towards the clients.

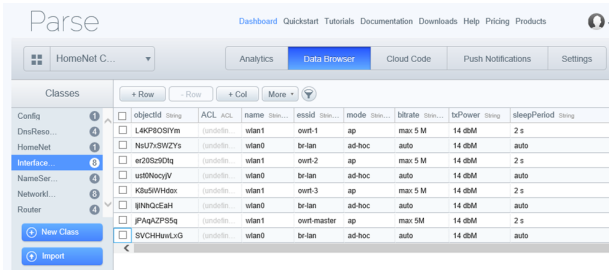

Figure 3: Parse Cloud-based platform

To manage the home network, we used Parse [6], a popular Backend-as-a-Service (BaaS) cloud platform, to host the remote controller. The configuration parameters of home network devices are represented as data objects on Parse as depicted in Figure 3. Parse provided several features useful for our prototype, such as a cloud-based data store, user management, user role based access control, push notifications, and support for cloud-hosted code. Our prototype uses Parse JavaScript SDK to provide a web GUI for the users of the cloud-based management service. This GUI allows users to add and remove managed devices, view and set configuration parameters of a network device, and change the set of configuration parameters currently used by all network devices.

Figure 4 shows our design for storing versioned configuration data in Parse. Several named configurations of the home network devices can be stored in the cloud, maintaining current as well as previous versions of configurations. Each configuration comprises the parameters of all home network devices being managed. When there are changes to a configuration and the changes have been committed, a new version of the configuration is created. The set of previous versions of each configuration allows reverting to a previous version of the network configuration if needed. New named configurations can be created as needed, either using a previously stored configuration as a template or by taking a snapshot of the current state of home network device configurations.

Parse also supports a REST based API that could be used for providing access to parts of the Homenet configuration by Internet-based automation services such as If This Then That (IFTTT) [7]. This provides the ability to build management apps that can configure and manage the home network via Parse, based on policy or context-based events triggered from IFTTT recipes (such as powering down non-essential radio interfaces based on time, user presence, or power savings profiles). An initial prototype of the local controller implemented in Node.js is currently running on a Linux PC and

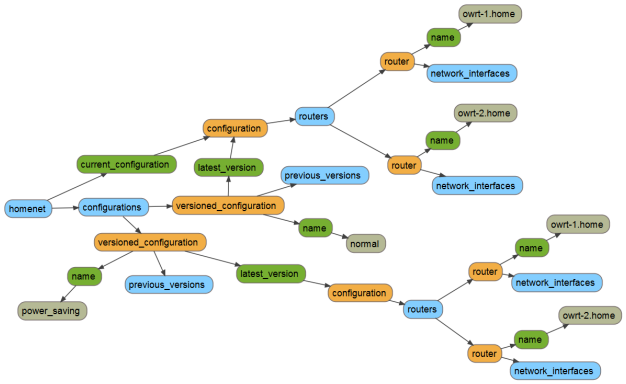

Figure 4: Versioned configuration data

uses the Parse JavaScript SDK to access the home network configuration data stored in the cloud. It then executes management commands on each router over SSH. Work is being undertaken to instead use an Android-based smartphone as the local controller that receives push notifications from Parse. The phone then uses REST-based method calls using CoAP [8], or RESTCONF [9]. CoAP is the basis for device management in the OMA Lightweight M2M [10] specifications, while RESTCONF is a RESTful approach towards using NETCONF [11] to manage the access points.

V. Security Issues

To allow collaborative management of the home network by the different stakeholders, it should be possible to define access rights to different subsets of network configuration parameters for groups of users according to their user role. The basic rule we wish to adhere to is to ensure that all modifications to the network are done via the cloud, and that executing these changes to the residential network via the local controller can only be rendered possible with explicit authorisation of the transaction by the home network owner. To accomplish this, we rely on a two-phase authentication and access control security model which are closely tied with each other.

In the first phase, authentication and access control to the data in the cloud is addressed. In this phase, the owner of the network would be free to assign roles and time-based access to various types of apps (or providers and users) accessing the cloud-based data. This allows trusted users to read and write the resource graph of data objects representing the configuration parameters of home network devices. Different views and access rights to the resource graph can be provided on a continuous or time-limited basis according to arbitrarily defined user roles. Certain roles, such as the primary Homenet user, could have full read-write access to all configuration parameters, while other users may be limited to read-only access or have no visibility to parts of the network configuration at all. An external service-specific controller such as an Internet-based automation service could also be provided access to selected parts of the network configuration via the cloud.

Once a valid management operation is performed in the

cloud, the local controller is notified, and successful execution of the operation is achieved by the local controller onto the residential access points upon successfully completing the second phase of authentication and access control. For this phase, an AAA-based mechanism is employed, in which the RADIUS protocol [12] is heavily used. Each home contains a RADIUS server capable of authenticating local users against provided credentials such as passwords, for obtaining network connectivity from the home network. However, when the local controller receives a request to update network settings, it can escalate its privileges from obtaining connectivity, towards performing network administration, by supplying credentials provided to it from another federated RADIUS-based realm, such as a security service provider (which could be the network operator, or a third party service provider). Successfully authenticating against these credentials would allow the local controller to be recognised as a valid executor. In our implementation, our initial strategy for the local controller has been to obtain an assurance of its identity by the security service provider, which informs the home RADIUS server what the device being authenticated is allowed to do.

VI. Conclusions and future work

In this short paper, we presented our active work-in-progress architecture, design, and implementation experiences in providing a new solution to allow expert external assistance to co-manage residential home networks of the future, without the need to have end-to-end network or physical connectivity to each element that needs to be configured and controlled in a home. Our initial tests and results appear promising as valid solutions of using a cloud-based controller for the management of, among others, Homenet-compliant home networks, without breaking any compatibilities. The connected home is becoming the technological focal point for intelligent control and communications systems, as well as consumer and personal electronics and advanced sensoring and actuating components. However, it is commonly assumed that it is the sole responsibility of the home owner to manage his network, which is a daunting prospect. Our solution offers a clear separation of concerns for the multiple stakeholders interested in making the smart home a success: The owner, the members of his family, the network operator, the cloud service providers and various third party experts. In so doing, new business models and revenue streams are created, while allowing service providers access and management capabilities to govern any devices they own residing within the home.

Apart from obtaining expert help, there are several other advantages to our approach. For example, a home network operational state and properties of the routing and switching elements can be preserved easily in the cloud. As residential access points tend to be commodity, cost-effective equipment, this approach allows easy rectification and replacement of defective routers, by restoring existing network configurations into new equipment. Also, upgrading network equipment in the home to take advantage of new technologies can be performed without much consternation.

Communication between the cloud and the local controller is completely REST-based. Uplink disruptions, as well as disruptions between the local controller and the routers, do not affect the actual operation of the home network. Once the uplink resumes, the local controller synchronises any changes or new policies with the cloud and applies them to the home network. In future, we aim to deploy RESTCONF-based communication between the local controller (i.e. smartphone) and the residential network elements. This allows easy interworking and integration with the Web of Things, allowing the formulation of intelligent decisions and sophisticated policies by obtaining contextual and geophysically relevant data from external web-based data sources. This results in fine-tuned policies for network performance towards various energy profiles, bandwidth control, data aggregation and traffic routing.

The architecture also considers proper authentication and role-based as well as time-limited access control as an important facet. While we are using RADIUS-based authentication and access control using passwords, in the future we aim at investigating SIM-based authentication solutions [13] that could identify the roles a owner's smartphone can fulfill.

Finally, the solutions proposed and studied in our research are highly scalable, allowing not only management of home routers, but also other types of constrained IoT-like nodes such as sensors and smart consumer appliances that allow REST-based resource retrieval and manipulation.

VII. Acknowledgements

This work is funded by the Finnish Digile IoT Programme.

References

[1] T. Chown, Ed., J. Arkko, A. Brandt, O. Troan and J. Weil, "IPv6 Home Networking Architecture", IETF Internet draft, work in progress, July 4, 2014; http://tools.ietf.org/html/draft-ietf-homenet-arch-17.

[2] J. Chroboczek, The Babel Routing Protocol, IETF RFC 6126, Apr. 2011; http://tools.ietf.org/html/rfc6126.

[3] R. Coltun, D. Ferguson, J. Moy and A. Lindem, Ed., OSPF for IPv6, IETF RFC 5340, July 2008; http://tools.ietf.org/html/rfc5340.

[4] G. Malkin, RIP Version 2, IETF RFC 4822, Nov. 1998; http://tools.ietf.org/html/rfc2453.

[5] M. Stenberg and S. Barth, "Home Networking Control Protocol", IETF Internet draft, work in progress, June 25, 2014; http://tools.ietf.org/html/draft-ietf-homenet-hncp-01.

[6] "Parse - The complete mobile application plaform", Oct. 5, 2014; http://parse.com.

[7] "IFTTT: Put the Internet to work for you", Oct. 5, 2014; http://ifttt.com.

[8] Z. Shelby, K. Hartke and C. Bormann, The Constrained Application Protocol (CoAP), IETF RFC 7252, June 2014; http://tools.ietf.org/html/rfc7252.

[9] A. Bierman, M. Bjorklund, K. Watsen and R. Fernando, "RESTCONF Protocol", IETF Internet draft, work in progress, Feb. 13, 2014; http://www.ietf.org/archive/id/draft-bierman-netconf-restconf-04.txt.

[10] "Lightweight Machine to Machine Technical Specification", Candidate Version 1.0 - 10 Dec 2013, Open Mobile Alliance, OMA-TS-LightweightM2MV1_0-20131210-C; http://www.openmobilealliance.org.

[11] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., Network Configuration Protocol (NETCONF), IETF RFC 6241, June 2011; http://tools.ietf.org/html/rfc6241.

[12] C. Rigney, S. Willens, A. Rubens, and W. Simpson. Remote authentication dial in user service (RADIUS), IETF RFC 2865, Jun. 2000; http://tools.ietf.org/html/rfc2865.

[13] H. Haverinen, Ed. and J. Salowey, Ed., Extensible Authentication