Nomadic Mobility between Smart Homes

Raihan Ul Islam, Mischa Schmidt, Hans-Joerg Kolbe
NEC Europe Ltd
Kurfürsten-Anlage 36
69115 Heidelberg, Germany

Karl Andersson
Pervasive and Mobile Computing Laboratory
Luleå University of Technology
SE-931 87 Skellefteå, Sweden

Abstract—Powerful, user-friendly mobile devices and cost-efficient wireless access technologies have lately changed the landscape for smart home environments to a large extent. Developments in the media landscape with large flat screens, new capturing devices, and large digital media libraries have also changed the way smart home environments are used. This paper presents and evaluates an architecture for nomadic mobility in such environments where end-users, by authenticating their terminals with a node in the home or visited environment using the infrastructure provided by the operator, easily can gain access to various types of resources at home while roaming to other people’s home networks.

Keywords—Mobility; Smart Home Environments; Fixed Mobile Convergence; Media delivery; AAA architecture

I. INTRODUCTION

With the advent of new smartphones and tablets on one hand, and various types of media devices like large flat screens, new capturing devices, and large digital media libraries on the other hand, new exciting smart home applications are becoming increasingly popular. Cost-efficient and easy-to-install wireless networking solutions are also important components when building advanced multi-media home services and applications. Last, but not least, standardization efforts like OSGi, Java, UPnP, and Radius have over the past years paved the way for vendor independence and compatibility across platforms. As a result, users can today easily access media within their local home environments using off-the-shelf devices. Access to game consoles, TV sets, and locally stored media archives are becoming widespread also for the casual users.

However, users also desire strongly to share media they have stored in their home network devices with friends in a user friendly, convenient and secure way. We believe that the network operator who already has established relationships with end customers and controls the network infrastructure can play a crucial role to address this need by offering a service facilitating the media sharing for mobile users. In particular, this paper presents and evaluates an architecture for nomadic mobility in smart home environments based on AAA (authentication, authorization and accounting) mechanisms in conjunction with media proxies aggregating and presenting content to any type of HTTP-enabled device. End-users can, by simply having their mobile devices authenticate with a visited node, easily gain access to various types of resources at home while roaming to other people’s home networks. Following the definition of nomadism in [1], we focus on a mobility concept where service sessions are disrupted, when the user moves to another access point.

The security mechanisms make use of a trusted relationship between the involved home gateways and the operator’s AAA infrastructure. While Section II of our paper surveys related work, Section III presents relevant technologies and ongoing standardization efforts. Section IV presents the proposed architecture and a prototype developed. Section V presents results and conclusions, while Section VI concludes the paper and indicates future work.

II. RELATED WORK

Belimpasakis et al. [1] proposed a solution that allowed home hosted content, located on home PCs or UPnP media servers, to be offered to remote clients, for consumption. A proxy residing in the home network exported multimedia content to a web syndication feed following the Atom protocol. Remote clients could access those proxy servers.

Kim et al. [3] proposed a methodology to provide services for accessing and sharing various media contents securely being distributed over consumer electronics (CEs) in the home network. The authors proposed the DLNAProxy System (DPS) architecture that helped to gather various media information available from distributed A/V devices in the home and to share the media contents across the public IP network via established secure channels.

Mahdi et al. [4] described a new service that allows multimedia sharing between UPnP terminals connected to remote networks. The service grants the confidentiality of users’ content since it is still stored in the home network. Their approach uses the IP Multimedia Subsystem (IMS) framework to establish a secure HTTP session between remote devices. Similarly, Fasbender et al. [5] described a similar system for remote access to home networks using IMS based Home Gateways.

Kim et al. [6] proposed a methodology to provide an integrated multimedia services framework in the home network. To do so, they defined the requirements of a home media server, and implemented its functionalities as a gateway for establishing connections between the home and external networks. The home media server pursued not only the integration of home network middleware technologies that allow automatic control and sharing with various Consumer Electronics (CEs) and A/V devices, but also intended to provide context based intelligences to the multimedia services for ubiquitous home environments.
Valtchev et al. [7] presented an implementation of the OSGi standard that enhanced the standard and integrates many existing home protocols and home networks. The enhancement extended the ideas behind the OSGi specification, allowing its direct application to real-life situations. Special emphasis was placed on realizing an effective and realistic gateway management system. The architecture presented was applied in several pilot projects.

Huang et al. [8] introduced MyHome, a framework for smart homes by which household information is all at a fingertip. Through adopting Message Oriented Middleware (MOM) and Open Service Gateway Initiative (OSGi) technologies, MyHome offered reliable automatic operations, fault tolerant and configurable home automation, high extensibility and large scalability. The proposed system was designed in terms of a residential gateway, MyServer, and an Internet accessible GUI, MyIcon, and MyMobile. The gateway was used to provide services for home security, inventory tracking, facility management, GPS location recording and family care.

III. TECHNOLOGIES AND ONGOING STANDARIZATION ACTIVITIES

This section introduces and describes technologies and standards relevant to the use case laid out in Section I.

A. Programming/Execution Environment, Home Gateway

The Open Services Gateway initiative (OSGi) [9] framework offers a dynamic system platform for modular Java based software components. The framework offers APIs for component life cycle management and a service registry via which components can offer their services to other components or consume services from other components.

The OSGi Alliance evolved its specifications beyond the original focus of service gateways which are now used in a wide range of applications on various platforms and environments.

In this work, we used the NEC Home Service Enabler as basis for our implementation which provides an OSGi environment.

B. Media Server Control in Home Networks

For media server discovery and media delivery in home networks the Universal Plug and Play (UPnP) [10] standard of the UPnP Forum uses a range of networking protocols. It permits networked devices, such as personal computers, Internet gateways and even mobile devices to seamlessly discover and use services for data sharing, communications, and entertainment. In essence, UPnP uses the Internet Protocol Suite (TCP/IP), HTTP, XML and SOAP for service discovery and consumption. For audio and video services, the extension UPnP AV was specified, which is referenced by other organizations including the Digital Living Network Alliance (DLNA) Networked Device Interoperability Guidelines, the International Electrotechnical Commission IEC 62481-1, and the Cable Television Laboratories Open Cable Home Networking Protocol.

C. Media Delivery and User Interface

Media delivery is today often handled using standard web technologies such as HTML over HTTP. This way, traversal of middle boxes like NATs and firewalls is smoothly handled. The new version of HTML, HTML5, together with its new set of Javascript APIs also allows for handling media directly in the web browser without any need for installation of third party plugin software such as Adobe Flash or Microsoft Silverlight.

The HTTP protocol is also used for file transfers quite frequently. Furthermore, using dynamically generated HTML by OSGi software in HTTP servlets is yet another common way delivering services to end-users.

D. Authentication, Authorization, and Accounting (AAA)

Authentication, Authorization, and Accounting (AAA) refers to a security architecture which enables control over which users are allowed access to which services, and account them for resource usage. In the industry, two network protocols providing this functionality are particularly popular.

RADIUS (Remote Authentication Dial In User Service) [11] provides AAA for devices to access and use a network service. It is a client/server protocol using UDP/IP as transport. RADIUS is based around the concept of Attribute Value Pairs (AVPs) to carry data. AVPs are extensible due to allowing vendor-specific AVPs to be carried. RADIUS is widely supported in the industry, e.g. by Internet Service Providers to manage Internet access of customers.

Like RADIUS, Diameter provides AAA functionality, but uses TCP or SCTP instead of UDP and can in principle be seen as an evolution (although not backwards compatible) of RADIUS. Diameter [12] is like RADIUS extensible by allowing applications to extend the base protocol. However, Diameter is conceptually more advanced through better scalability, by supporting network layer security through IPsec [13] or TLS [14] and a larger address space. While RADIUS is widely deployed in fixed-line networks and also part of the WiFi alliance’s specification on hotspots providing IEEE 802.1X [15] functionality, Diameter’s domain is the mobile network defined by the 3rd Generation Partnership Project (3GPP).

E. Authenticating the Mobile Device

For authenticating the mobile device at the visited home, various candidate technologies such as the IEEE 802.1X standard and Captive Portals exist.

IEEE 802.1X provides an authentication mechanism to devices wishing to attach to a LAN or WLAN with support built-into many popular operating systems. Typically, on detection of a new device (in our case the mobile, referred to as supplicant), the port on the network switch (typically a Home Gateway, referred to as authenticator) is enabled and set to an “unauthorized” state. In this state, only 802.1X traffic is allowed and all other traffic is dropped. Then, the supplicant and authenticator exchange layer 2 authentication traffic for EAP negotiation. The authenticator then initiates a RADIUS exchange with the RADIUS AAA server. Upon successful authentication, the authenticator sets the port to the
"authorized" state and normal traffic is allowed. In case of a failure to authenticate, the port remains in the "unauthorized" state. When the supplicant logs off, the authenticator sets the port back to the "unauthorized" state, effectively blocking non-EAP traffic.

An alternative approach to authenticate devices to a network relies on the so-called Captive Portal. This technique forces a device to first authenticate at a special web page (e.g. with username and password credentials entered in the device’s web browser) prior to allowing access to the Internet or other network services. This is done by intercepting all data traffic, and dropping all data traffic but HTTP traffic, which is redirected to a web portal for the authentication. Captive portals are commonly encountered at many Wi-Fi hotspots, and can be used to control wired network access as well.

There are multiple ways of forcing the device’s web browser to the captive portal, e.g. by directing all HTTP requests to the portal page using DNS and using the HTTP 302 response to redirect the browser to the originally requested web page upon successful authentication. Other alternatives using redirection mechanisms based on plain IP routing or based on DNS also exist. Despite the fact that we used a captive portal authentication mechanism for the roaming device, in a future development we will use 802.1X based authentication that will provide a seamless way to connect to the visited network without any user interaction.

**F. Standards**

The seamless authentication of roaming WiFi devices is part of multiple specifications in the standardization community. While the WiFi alliance’s WPA specifications already include a RADIUS client inside a hotspot, just recently the Broadband Forum and the 3GPP teamed up to develop a solution for fixed mobile convergence (FMC) that provides seamless mobility between the LTE macro network and local WiFi or femto cell accesses [16]. Our work goes beyond simply authenticating devices.

For remote access, the Home Gateway Initiative has published recommendations on how to achieve connectivity between home networks making use of the IMS [17]. ETSI TISPAN has later on standardized the solution [18]. None of this work included a service- and media-aware proxy functionality.

**IV. PROPOSED ARCHITECTURE AND VERIFICATION PROTOTYPE**

For distributed media sharing with centralized security and support mobility of users we propose a system based on application layer media proxies. Figure 2 illustrates the basic network architecture for the system.

![Figure 2. The proposed system architecture](image)

Each home will have a Home Gateway (HGW) device separating the Operator IP network and the user’s home network. In each home there will be different devices like IP
The communication between the HGWs uses the HGWs’ public IP addresses and the home network devices communicate with private IP addresses.

The system is designed in a modular fashion and implemented on carrier grade home gateways using OSGi. As illustrated in Figure 3, its four main components are located on the HGW.

1) RADIUS Client: The main purpose of this component is to communicate with the AAA server to authenticate and register the HGW towards the Operator as well as authenticating User A’s device. Further it receives User A’s HGW address, keeps track of the visiting devices and the associated authentication token received from the AAA server.

2) Multimedia Portal: This component is responsible for communicating with the media server in the local home network using UPnP. Furthermore, it provides a web portal to devices connected with the HGW displaying the media items available in the home itself as well as media items in remote homes made available through our system.

3) Web Proxy: In HGW A, this component is using XML via HTTP and provides a list of media servers as well as media items to HGW B by querying the Multimedia Portal. The Web proxy hides the internal network from the external network by indicating the media address as being the public HGW A address. Due to hiding the internal network, the component also informs the Media Proxy component how to proxy incoming requests for media items to the internal media server(s). In the visited HGW B, the Web Proxy queries HGW A for media servers and media items using HTTP. To show the eligibility of the request, HGW B sends the authentication token it received together with HGW A’s address from the RADIUS client component along with this request. Upon reception of the media list from HGW A, the Web Proxy component rewrites the media item links so that they point to the local Media Proxy component and gives the media item list to the Multimedia Portal. At the same time, the Web Proxy instructs the Media Proxy also how to proxy the media item links to HGW A.

4) Media Proxy: In HGW B, this component deals with requests for media received from local devices as indicated by the rewritten links of the Web Proxy. The Media Proxy redirects the media requests to HGW A and enriches each request for media with the authentication token received from the RADIUS client component securing the overall system communication. In HGW A, the Media Proxy component receives media requests, verifies the authentication token and proxies the media requests to the actual media server(s) in Home A.

To verify our prototype implementation, we set up an infrastructure (shown in Figure 4) consisting of a high-end PC with two network interface cards (NIC) and two home gateways (HGW). The HGWs and one of the PC’s NICs are connected with a “public” IP network, receiving IP addresses of the subnet 10.15.254.0/24. The PC is hosting two virtual servers. One virtual server is configured as AAA server using...
the “public” NIC. The AAA server is running FreeRADIUS [19] installed on Ubuntu OS. The other virtual server is configured as Media server for Home B and thus the second NIC is connected to the private IP network of Home B. It also has Ubuntu installed and uses the XBMC [20] media server software. This virtual server’s internal NIC is bridged with the NIC connected to Home B and thus the two virtual servers are effectively separated. The two HGW devices will act as home gateways for homes A and B and run our prototype software as described. Mobile A1 is a common smartphone with a standard Google Chrome web browser to authenticate at the captive portal of HGW B. An Android Tablet Device represents the device accessing the Media Portal and consuming the media of Home A.

V. RESULTS AND CONCLUSION

In this paper, we propose a system for smart, user friendly way of media access in cases of nomadic user mobility relying on operator security systems that reuses existing infrastructure and protocols. This way, it is possible to deploy this system concept with minimum effort and cost, e.g. without relying on IMS as [4][5]. We used an application layer media proxy for remote accessing instead of commonly used layer 3 approaches as mentioned by Kim et al. [3]. This opens opportunities for any HTTP enabled device for media access using our system. It also allows for full control of services in the application layer, enabling e.g. content based charging capability, policy implementation and/or parental control. For ensuring security via a token mechanism and for sharing connectivity information among the HGWs, devices and the AAA server we used vendor specific AVPs carried in Radius. It is noteworthy that our mechanism only adds one extra Radius CoA message to HGW A for informing the security token when compared to existing FMC message flows as discussed in the state of the art [16]. The security token is generated by the operator infrastructure and is used to authenticate access requests of HGW B at HGW A. As proposed in Mahdi et al. [4] the UPnP terminals are connected to remote networks, however our system hides home A’s UPnP terminals (their number and their IP addresses) from the remote network of home B along with the UPnP devices of home B, thus and providing a single interface for media access.

Our user interface is based on HTML, CSS3 and Javascript which ensures similar and thin interface for all type of devices (like smartphones and tablets) instead of using heavy technology like Java applets [7]. Moreover, our prototype is compatible with upcoming standards in the FMC field [16].

Finally, our approach inserts media proxies located within the HGWs in the communication between the home networks, resulting in a decentralized media routing solution. Since we reuse RADIUS messages that are already used in FMC scenarios for authenticating nomadic mobile devices when visiting home networks for a) sending network connectivity information, and b) the security token to the visited home network and only add a single Radius CoA message for communicating the security token to HGW A, scalability impacts on the existing infrastructure are marginal.

VI. FUTURE WORK

In the future, we will investigate QoS related issues with respect to the proposed HTTP based way of media sharing. We will also consider developing a decentralized mechanism for authentication and connectivity among homes instead of relying on the central AAA node. Further we will investigate the impacts of encrypting the communication between the home networks.

ACKNOWLEDGMENT

This work has partially been supported by the Nordic Interaction and Mobility Research Platform (NiMo) project [21] funded by the InterReg IVA North program.
REFERENCES


