Secure and Scalable Multimedia Sharing between Smart Homes*

Raihan Ul Islam[1], Mischa Schmidt[2], Hans-Joerg Kolbe[2], and Karl Andersson[3†]
[1]*TU Darmstadt, Hochschulstrasse 10, 64289 Darmstadt, Germany*
[2]*NEC Europe Ltd, Kurfürsten-Anlage 36, 69115 Heidelberg, Germany*
[3]*Pervasive and Mobile Computing Laboratory*
Luleå University of Technology, SE-931 87 Skellefteå, Sweden

Abstract

The smartphone revolution together with cost-efficient wireless access technologies has lately changed the landscape for smart home environments to a large extent. Moreover, large flat screens, new capturing devices, and large digital media libraries have also changed the way smart home environments are used. We present and evaluate an architecture for multimedia sharing in such environments. End-users can, by authenticating their terminals with a node in the home or visited environment easily gain access to various types of resources at home while roaming to other people's home networks. This is achieved by using the infrastructure provided by the operator.

Keywords: Mobility, Smart Home Environments, Fixed Mobile Convergence, Media delivery, AAA architecture, Security, Scalability, Fault Tolerance.

1 Introduction

Users desire to share media stored in their personal networked devices with others in a convenient and secure way. We believe that the network operator can capitalize on this by offering a media sharing service for mobile users. In [1] we presented an architecture for sharing media in the context of nomadic mobility based on AAA (authentication, authorization and accounting) mechanisms. We implemented this on OSGi enabled Home Gateways by using HTTP media proxies aggregating and presenting content offered by UPnP media servers to any type of HTTP-enabled device – regardless of its location. This effectively allowed end-users to easily gain access to various types of resources at home while roaming to other user's networks.

The key technologies being used in our solution include OSGi (Open Services Gateway initiative), RADIUS (Remote Authentication Dial In User Service), and UPnP (Universal Plug and Play). OSGi implements a complete and dynamic component model and forms a modular system and service platform. Typically reboots are not needed when applications or components are installed, started, stopped, updated, or uninstalled. Remote management of these actions is supported.

RADIUS is a client/server networking protocol providing centralized AAA and runs in the application layer using User Datagram Protocol (UDP) as transport.

UPnP, primarily intended for residential use, is a set of networking protocols that permits networked devices, such as PCs, printers, access points, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment. UPnP is an extension of plug-and-play allowing for dynamically attaching devices directly to a computer. UPnP devices are plug-and-play so that when connected to a network they automatically establish working configurations with peers.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 5, number: 3, pp. 79-93

*The system discussed in this paper was presented at the 4th IEEE Globecom International Workshop on Mobility Management in the Networks of the Future World (MobiWorld, December 2012) [1].

†Corresponding author: Tel: +46-910-585364, Email: karl.andersson@ltu.se

This article discusses scalability, security and fault tolerance aspects of the architecture we presented in [1]. The requirements for scalability, fault tolerance and security of our solution are considerable as our solution proposes to reuse critical operator infrastructure, in particular the operator's servers for AAA.

The remainder of this article is structured as follows: Section 2 surveys related work, Section 3 briefly summarizes the solution presented in [1]. Section 4 then discusses scalability characteristics, security considerations and fault tolerance aspects of the architecture and our developed prototype. Subsequently, Section 5 summarizes our discussions.

2 Related Work

For a description of related work in the field of remote multimedia access we refer to the State of the Art described in our earlier work [1].

Wu et al. [2] propose a service-oriented architecture (SOA) for smart-home environments, based on Open Services Gateway Initiative (OSGi) [3] technology. Similar to our work [1], this architecture is a Peer-to-Peer (P2P) model based on multiple OSGi platforms. Inspired by Wu et al we discuss Fault Tolerance considerations regarding the different components deployed in our solution in section 4.2.

Both Wu et al. [2] and Lin et al. [4] describe scalability aspects of their OSGi based architectures considering network traffic and computational load induced by their proposed systems. Given the relatedness of our work [1] to these systems, we also consider scalability aspects but – taking into account findings of [5] as well as the insight that in our work only a small fraction of the overall traffic converges at central points in the Operator network, the AAA infrastructure – we limit our focus in section 0 on network traffic with respect to AAA.

Hirsch et al [6] describe a service aware framework for designing context-aware ambient services. In their proposal, different communication standards are wrapped by a service execution engine unifying access and service provision across service domains. Basic building blocks are provided for security, multi-modal interaction, and management. The proposed framework lacks the feature of hiding the local network from operator network and also the nomadic mobility of user's device.

Fan et al. [7] describe a service middleware used for faster and more efficient development and runtime support of adaptive multimedia services in upcoming 4G environments. By using the OSGi technology the authors provide an interoperable infrastructure for efficiently building, provisioning, and managing mobile multimedia services. But this will cause the operator to add additional node to the network, which might bring additional cost. It might also cause integration problem with other nodes of the network.

Brewka et al. [8] propose a solution on resource allocation within home and access networks. The proposed inter-domain QoS signaling enabled the initiation of the QoS provisioning in the home and access from the end device in users home. The home network considered was UPnP-QoS enabled while the access network was GMPLS based. The authors proposed and implemented an interface between different network segments allowing for end-to-end QoS establishment. QoS parameters and mechanisms were presented in both UPnP-QoS and GMPLS. Also, the authors investigated the complexity of their proposed solution and presented implementation results. In the test scenario, it seems the setup time was comparatively higher. This might affect the use case for user initiated resource allocation.

3 A Solution for Nomadic Mobility between Smart Homes

This section summarizes the solution we introduced in our earlier work [1] to address the use case of Section 1.

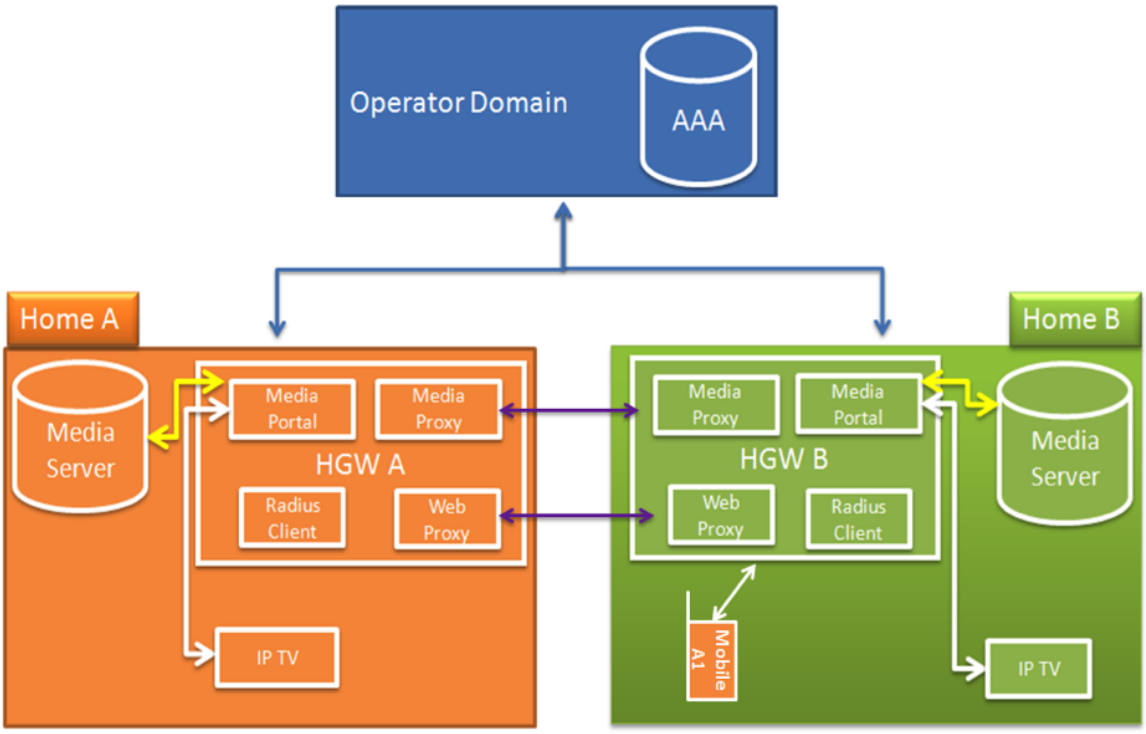

Figure 1: The system architecture

3.1 Architecture and Technologies

As shown in Figure 1, in each home an OSGi enabled Home Gateway (HGW) device separating the Operator IP domain and the user's home network has been deployed, running our prototype OSGi based software consisting of four conceptual parts: Media Portal, Media Proxy, Web Proxy and AAA Client, as described in [1]. The HGW devices effectively hide (and protecting) the IP enabled multimedia devices in each home from the outside world though firewalling and private network addresses.

When user A visits home B (in Figure 1), the "visited home", user A's mobile smart phone ("Mobile A1") will attach to the home gateway ("HGW B") of the visited home. Subsequently, Mobile A1 will authenticate via HGW B with the Operator's AAA server relying on standard technologies such as captive portals, 802.1x authentication mechanisms, RADIUS [9], etc. Subsequent to the successful authentication of Mobile A1 our solution employs a sequence of messages involving RADIUS, HTTP and UPnP [10] protocols in order to grant access to home B's IP enabled devices via HGW B to the IP enabled media servers of home A via HGW A. Figure 2 shows the conceptual flow of information as proposed in our earlier work [1].

3.2 Our Solution in Light of Recent Standardization Activities

The authentication of Wi-Fi devices is part of multiple specifications in the standardization community. While the Wi-Fi Alliance's WPA specifications already include a RADIUS client inside a hotspot, mainly to enterprise scenarios, the CAPWAP protocol and architecture [11], [12] leverages this for public Wi-Fi

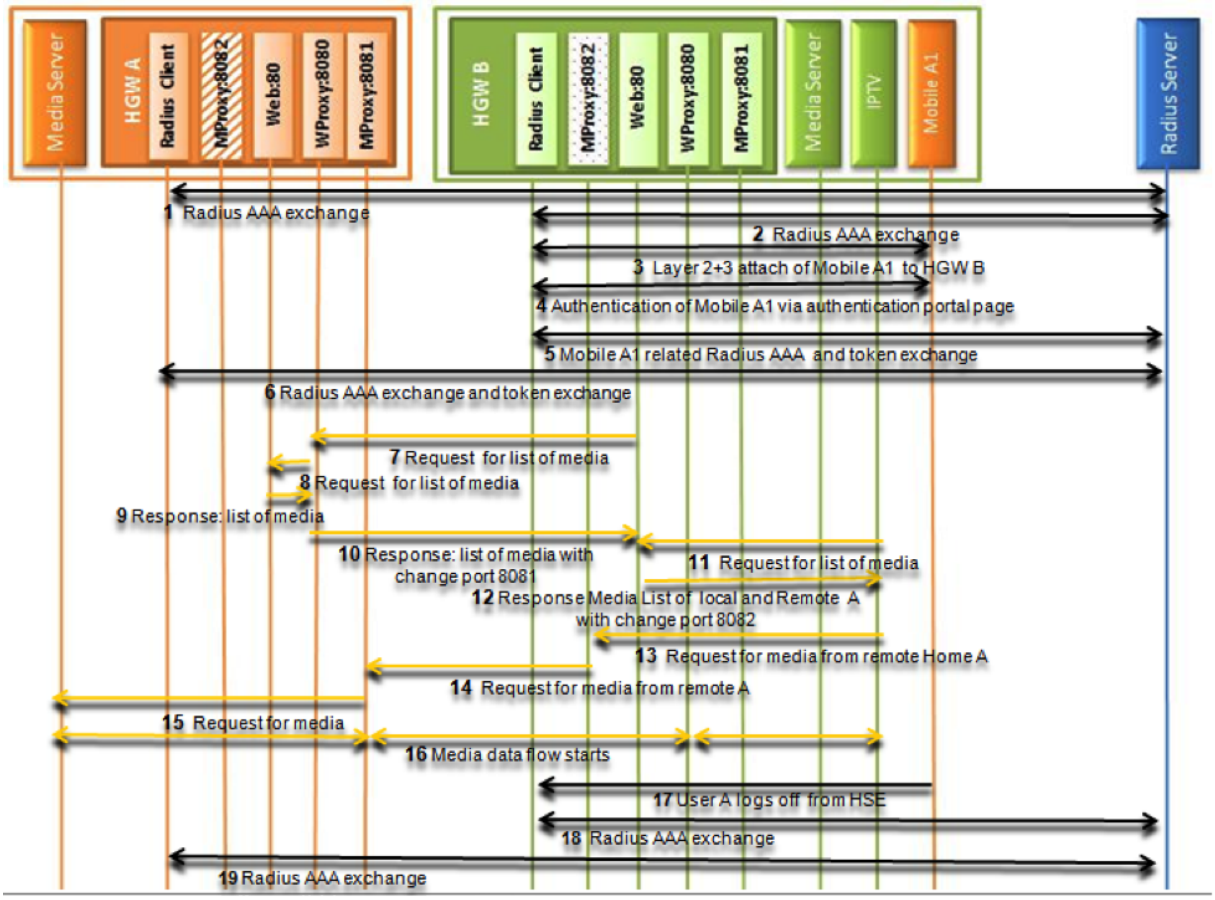

Figure 2: The message flow of media sharing using application layer media proxies

access use.

Recently, the Broadband Forum and the 3GPP teamed up to develop a solution for fixed mobile convergence (FMC, see [13]) that provides seamless mobility between the LTE macro network and local Wi-Fi or femtocell accesses [14]. In the trusted interworking scenario (S2a method), RADIUS is used as authentication protocol for 3GPP devices roaming into customer premises networks, proxying EAP over RADIUS (defined in [15]and 3GPP WLAN interworking standards [16], [17], [18]). Details of this interworking procedure are currently being developed at the BBF and 3GPP.

Our work goes beyond simply authenticating devices as we also address authorization and possibly accounting (the other two A's of AAA). The BBF is currently discussing how to bring requirements from 3GPP interworking, CAWAP/public Wi-Fi and our extensions into a common standards document.

For remote layer-3 (IP) access to customer premises networks, the Home Gateway Initiative has published recommendations on how to achieve connectivity between home networks making use of the IMS [19]. ETSI TISPAN has later worked on standardizing the solution [20]. So far, none of this work went beyond a plain VPN-type access model or included a service and media aware proxy functionality as we developed in our work.

4 Discussion: Scalability, Fault Tolerance, and Security

This Section discusses our proposal in terms scalability, fault tolerance, and security. We indicate pros and cons of proposals in related work covered in Section 2 in Table 1.

Table 1: Comparison among Related Works

Related Work	Pros	Cons
Wu et al. [2]	This work proposes a service-oriented (SOA) peer-to-peer (P2P) architecture for smart-home environments. It is based on OSGi and mobile agent (MA) technology.	The proposed solution lacks nomadic mobility for users
Hirsch et al. [6]	This work describes a service aware framework for context-aware ambient services. It provides basic building blocks for security, multi-modal interaction, and management	The framework lacks the feature of hiding the local network from operator network and also the nomadic mobility of user's device.
Fan et al. [7]	This work describes a service middleware used for faster and more efficient development and runtime support of adaptive multimedia services in 4G environments	This will cause the operator to add additional node to the network. It might also cause integration problem with other nodes of the network.
Brewka et al. [8]	This work proposes a system for establishing QoS from Home Network to access networks	In the test scenario, it seems the setup time was comparatively higher which might affect the use case for user initiated resource allocation.

4.1 Scalability

4.1.1 General considerations on Computational Load and Network traffic

In this section, we investigate the scalability of our solution. Scalability considerations as for example formulated in [2], [4] typically consider both computational load as well as network traffic load of the different steps of the proposed solution induced at the different components. In our case, as shown in the high level message flow (Figure 2), there are three distinct phases:

1. Authentication of the mobile device in the visited home (AAA)
2. Media exchange between the home networks (HGW, in home traffic)
3. Termination of the service (AAA)

Phases one and three involve the operator AAA infrastructure where the authentication traffic of the different users and home networks converges. For phase two the media exchange phase of our

solution is handled in a peer-to-peer fashion between the HGWs directly, this phase is considered to scale very well[1]. Considering that for our prototype implementation the computational load at the HGW components only scales with the number of visiting/nomadic mobile devices in terms of HTTP proxy interactions as well as a small amount of XML parsing in case the devices browse the media portal, we consider the computational load at the HGW components to be negligible for modern OSGi enabled HGWs. As a consequence we argue that the centralized AAA infrastructure involved in phases one and three determines the scalability of our solution and thus we focus our further discussion on it.

According to [5], the computational load associated to AAA traffic at components involved is not limiting scalability when compared to the network traffic bandwidth required by the AAA interactions. We therefore focus our discussion of the AAA related phases on network traffic only as documented in Section 4.1.2.

Table 2 summarizes network traffic interactions of the different phases, abstracting from underlying communication protocols.

Table 2: Network interactions per component by different operations

	Operations	Interactions at components				
		Client	HGW A	HGW B	Media Server	RADIUS server
AAA operations	Client authentication request	1	1	1		2
	Client log off request	1	1	1		2
Media sharing	HGW requests media list from Media Server		1		1	
	In-home device requesting media list	1		1		
	HGW B requests media list from HGW A		1	1		
	In-home device requesting media from local Media Server	1			1	
	In-home device requesting media from remote home network	1		1		
	HGW B requesting media from HGW A		1	1		
	HGW A requesting media from local Media Server		1		1	

4.1.2 AAA Communication and Scalability

In this section we investigate the AAA related communication of our solution. We consider this to be of particular relevance to Operators as the AAA.

[1]While this phase is considered to be highly scalable, the available uplink and downlink bandwidth of both involved home networks has impacts on the Quality of Experience perceived in the visited home.

From Table 2 follows that per service invocation, i.e. per mobile device visiting a home network, two AAA interactions are triggered at the AAA server component. One for each involved HGW. Similarly, when the mobile device terminates the service, e.g. by leaving the visited home network or by explicitly signing off, two AAA interactions are triggered at the AAA server, one for each HGW. For a conservative reflection, we consider the two interactions per AAA interaction phase as additional load on the AAA server caused by solely our solution, although information for multiple similar services could be sharing one AAA message and effectively reducing the interaction overhead of our solution.

Considering our prototype implementation using (CHAP protected) RADIUS traffic between HGWs and AAA server, two messages are exchanged per interaction shown in Table 2. To convey information necessary to enable and protect(see the security discussion in Section 4.3) the media exchange between the home networks in a standards compatible way, we used vendor-specific RADIUS Attribute Value Pairs (AVPs) carrying data from the AAA server to the HGWs and vice versa. For service invocation we use the RADIUS Access-Request message as this is suitable to carry the visiting user's credentials. Upon successful authentication, a security token generated at the AAA server and the visiting user's home connectivity information are carried in the corresponding AAA server Access-Accept message to the visited HGW (HGW B). At the same time, in order to inform the visiting user's HGW (HGW A) of the security token and to prepare it to serve media to HGW B, a RADIUS CoA-Request with the respective information is sent to the HGW. This HGW in turn confirms the receipt with a normal RADIUS CoA-Ack message. In case of service termination triggered from HGW B, a RADIUS Accounting-Request message is sent to the AAA server, which responds with an Accounting-Response message. At the same time, HGW A is sent a new security token in a RADIUS Disconnect-Request (which HGW A confirmed in a Disconnect-Response) in order to prevent HGW A to serve future media requests from HGW B with the now outdated token.

Due to causing two AAA interactions (one with each involved HGW) per service invocation or termination, we believe our service makes efficient use of the scarce and critical resource AAA server in the operator network. Besides our solution benefits from the fact that RADIUS servers are highly scalable and widely used. For example, the AdvOSS AAA Server [21] is reported to handle between 2,000 and 3,000 requests per second, while the most spread RADIUS server software, the open source FreeRADIUS server [22], is reported to handle up to 1,000 requests per second.

For user authentication in order to invoke the service, our solution will require two RADIUS interactions. The first interaction (triggered by HGW B) consists of the RADIUS Access-Request and Access-Accept messages which have a message size of 120 bytes and 135 bytes respectively in our implementation. The second RADIUS interaction of the service invocation phase involves HGW A and consists of CoA-Request and CoA-Ack messages – in our implementation with a message size of 105 bytes and 62 bytes respectively. Therefore, in total 422 bytes of RADIUS traffic are exchanged for the service invocation in our proposed system. Note that message sizes may vary depending on various parameters such as username and password length or the domain names used.

For the user log-off interaction to terminate the service, also two RADIUS interactions are required. The first interaction (triggered by HGW B) consists of Accounting-Request and Accounting-Response messages. The size of these messages is 125 bytes and 62 bytes respectively in our implementation. The second interaction involves HGW A and consists of Disconnect-Request and Disconnect-Response messages with a size of 77 bytes and 62 bytes respectively in our implementation. Thus, the logout interaction in our experimental implementation totals to 326 bytes. Note again that message sizes may vary depending on various parameters such as username length or the domain names used.

4.1.3 Evaluation of Scalability

In order to evaluate the scalability of our proposed system we developed a simulation tool implementing a Poisson arrival process of AAA traffic. For the simulation we modeled an AAA server with 180 threads for handling incoming AAA messages and a message buffer size of 4,000 messages[2]. We chose these parameters in order to resemble a typical AAA server throughput limitation in the range of the capacities given in literature as documented in the earlier section. We simulated for different arrival rates λ = [1.0 ... 3.0] in 0.1 increments of λ. For each value of λ the simulation was iterated 100 times. Each simulation ran for 10 minutes, neglecting the first 5 minutes of simulation as system warm up time.

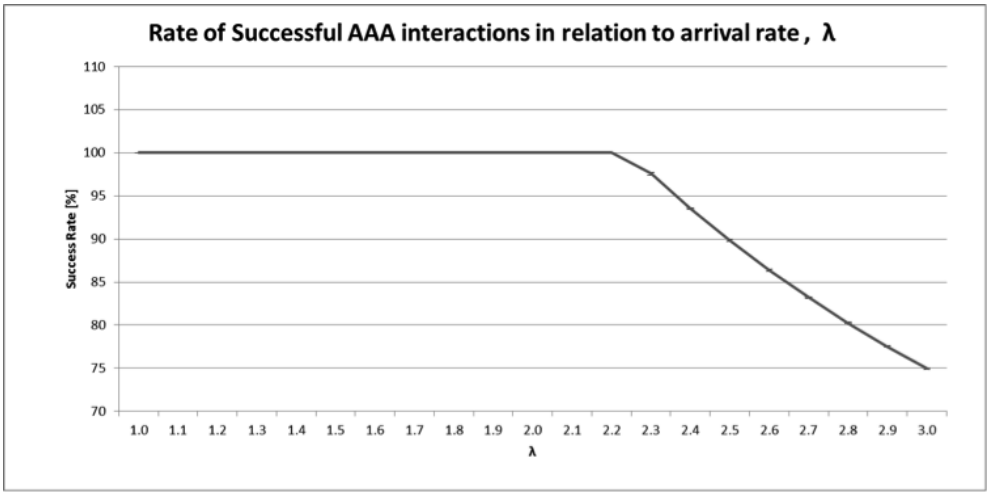

Figure 3: Rate of successful AAA interactions in relation to arrival rate, λ

As shown in Figure 3, the success rate of AAA message processing is constant at 100% up to λ=2.2 (equivalent to 2,200 AAA interaction per second). Beyond that the success rate declines. For λ=3.0 the average success rate is 75% with a standard deviation of 0.08%. Figure 3 also shows that the standard deviation of each set of 100 iterations per different simulation is very small – the maximum standard deviation of the rate of successful AAA interactions we observed was 0.14% for λ=2.3, i.e. just above the capacity limit of the modeled server.

Figure 4 displays the number of successful AAA interaction per second of each simulation. This is saturating between λ values 2.2 and 2.3 indicating the throughput limit of our modeled AAA server – experimental results show a capacity limit of the modeled AAA server at 2,247 AAA interactions per second.

To estimate the impact of our solution on the AAA infrastructure when facing real world mass scale events, we assume a situation where users authenticate with our service during a time window of e.g. 5 minutes – for example during 5 minutes before kick-off of a popular football match users will arrive. In this setting, using aforementioned server dimensioning and arrival process, our service would – theoretically – support 660,000 users being served by a single AAA server with a success rate of 100%[3].

[2]With these parameters we experimentally verified to serve approximately 2,000 AAA interactions per second – which is in the range of server capacities considered in section 4.1.2.

[3]Assuming an AAA server dimensioning of 2,200 AAA interactions/second * 300 seconds.

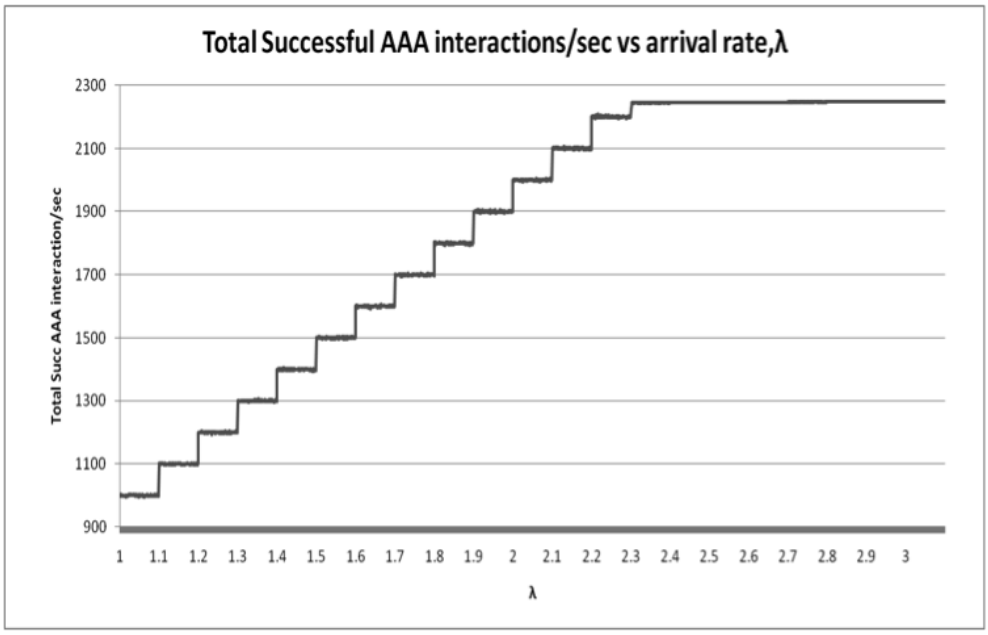

Figure 4: Total successful AAA interactions/sec vs. arrival rate, λ

4.2 Fault Tolerance

This section describes the effect of failures at different components of our solution and discusses possibilities of mitigating the effects of the failures.

4.2.1 Mobile Device

The role of this mobile device is to authenticate the nomadic user in the visited home. A failure of the device to invoke the chosen authentication mechanism (e.g. 802.1x or the mobile browser in case of a captive portal) will prevent the message flow shown in Figure 2 at the very start and the Operator unable to detect this failure. Consequently, the visited home will not receive media information about the visiting user's home. This type of fault can be mitigated by implementing multiple alternative authentication schemes into the mobile device and the HGW. Certainly, this way of mitigation implies a higher complexity and cost of the solution and will not be able to address critical failures of the Mobile Device itself.

4.2.2 OSGi Software on HGW

Our proposed software consists of four components as outlined in our earlier work. Each component is critical to the message flow shown in Figure 2. Therefore, if any of the components fails or the HGW itself fails, no media exchange is possible. However, each component failure implies slightly different effects:

- The AAA client authenticates the respective HGW with the operator, registers the communication addresses and ports for media exchange and also proxies the visiting mobile device credentials to the Operator AAA infrastructure. Without this component, no media exchange is possible due to lack of proper authentication at the Operator infrastructure. In case the visited HGW exhibits the failure, the operator is unlikely to be aware of HGW B or the fact that user A visited home B. If

HGW A failed, the Operator will not be able to indicate home A to HGW B as a source of media. The operator can only detect the failure of this component in case error reporting is implemented upon failure of the component.

- The Web Proxy and Media Proxy components act for the actual media information as well as media exchange between the home gateways. Thus, a failure of these will result in failure to communicate media information or provide media access. The Operator infrastructure will however have detected that a user A is nomadic and visiting home B. Thus, depending on the capabilities of the HGW infrastructure, potentially the Operator could take action to restart the failing components of the software solution, effectively hiding the failure from the user but causing a delay until media exchange is possible.

- The Media Portal provides a user interface to devices in the visited home. It is intended as the one-stop-shop for media consumption in a networked multimedia home and a failure of this component will cause the users being unable to browse and access the media of both home networks. The failure of this component can only be mitigated locally in the visited home network, e.g. by restarting the corresponding component on HGW B.

4.2.3 Operator Infrastructure

Failure of the operator's AAA infrastructure will prevent our solution from working as it will prevent the message flow shown in Figure 2 at the very start and thus preventing the entire service scenario. Unlike in the case described in section 4.2.1, the Operator is able to detect and act upon the failure of its (critical) infrastructure. Additionally this scenario may be seen as highly unlikely as it is assumed that Operator AAA infrastructure is carrier grade and fault tolerant.

4.2.4 Communication Failure

Yet another component that may fail is the communication between the mobile device and the HGW on the one hand, and the communication between the HGW and the Operator AAA infrastructure on the other hand. One may consider alternate solutions with multiple HGWs deployed at the customer premise both taking care of node failure of an individual HGW and the communication between the mobile device and the HGW. This scenario is, however, left as future work. Failure in the communication between the HGW and the Operator AAA infrastructure may be caused of the failure in the access or core network on the path from the HGW to the Operator AAA infrastructure. Such failures are beyond the scope of this study.

4.3 Security Considerations

This section discusses first security considerations of our work proposed in [1]. Further work is required with respect to an in-depth attack and threat model analysis.

Conceptually, in the service consumption there are three different phases as mentioned before:

1. Authentication of the visiting mobile device
2. Service Access
3. Service Termination

4.3.1 Authentication of the Visiting Mobile Device

As described in [1], our solution can draw from various candidate technologies such as the IEEE 802.1X [23] standard or Captive Portals to authenticate the mobile device at the visited home and the AAA system. We consider the use of these approaches as state-of-the-art.

4.3.2 Security of Service Access

After successful authentication of the visiting user's mobile device (Mobile A1) via the visited Home Network Gateway (HGW B), our prototype system secures media exchange between the users' home networks by means of a token generated in the Operator's AAA server and communicated to both users' home gateways using (presumably) secured AAA RADIUS communication. To enhance security further, the HGW B WAN IP address is also indicated by the AAA infrastructure to HGW A along with the token. Additionally, our prototype shares the identifier of user A used in the captive portal with HGW A for logging purposes. Since the Operator AAA infrastructure is critical infrastructure for the Operator, we consider this token issuing and distribution process as trusted. We see the possibility to generate the token at Mobile A1 (and communicating it to the AAA server during the authentication phase); however this would give rise to a systematic security risk: the visiting user (or its Mobile A1) might choose/generate weak tokens endangering its home network.

Subsequently, our HGW A will only allow accesses to media in home network A if the requests of HGW B carry aforementioned token to indicate the validity of HGW B's request. Further, HGW A verifies HGW B's WAN IP address as indicated by the AAA server beforehand. As our prototype system uses HTTP for the media access, we relied on HTTP URL parameters to indicate the token in service requests from HGW B to HGW A. At present the traffic between HGWs is not encrypted and we see potential to enhance the security of this phase in the following ways:

- Home Gateways A and B use a cryptographic algorithm to generate a token of validity themselves each time a request is sent from HGW B to HGW A. This algorithm uses a seed chosen by the Operator AAA infrastructure generated when mobile A1 authenticates in the visited home. In other words, the token currently generated in our prototype implementation plays the role of a seed for said cryptographic algorithm.

- The protocol to exchange media between homes A and B could be changed from plain HTTP into HTTPS or secured by an encrypted tunnel. The token generated by the Operator AAA server in our prototype implementation could become the key of the encryption process. We consider this as complementary to the use of aforementioned cryptographic algorithm.

One other potential point of critique, though not strictly speaking a security issue, is related to the question how much of the media (or more generally speaking, resources) of home network A should be accessible to users in home network B. Our current prototype implementation shares all media items via UPnP with home network B, but more sophisticated mechanisms are possible, depending on the service definition:

- Sharing only files following a specific naming convention or file type

- Sharing only specific sub folders of media servers

- Sharing only specific media servers

- Using Access Control Lists to explicitly identify which files can(not) be shared

Each of these approaches can further take into account the user's identifier in order to allow personalized media sharing.

To enhance security further, HGW A could request user confirmation from Mobile A1 when it receives HGW B requests. This interaction could be realized via HGW B or via other communication channels and may be required depending on the service definition at different levels:

- Require user confirmation on each interaction/request received at HGW A
- Require user confirmation per media server access within home network A
- Require user confirmation per media item accessed within home network A

4.3.3 Security of Service Termination

Once user A leaves home network B or explicitly signs off from the service portal page, our prototype implementation generates a new token in the Operator AAA server which is then shared with HGW A. Our software in HGW A then terminates active data transfers with HGW B associated to Mobile A1 and will not accept further requests from HGW B using the previously valid token. We consider this approach as sufficient to protect against replay attacks using previous tokens from a malicious HGW B.

Should however HGW B prevent Mobile A1 from signing off from the service portal page, our prototype system would not issue a new token, effectively allowing HGW B continued access to home network A. A possible approach to address this is to require interaction with Mobile A1 in intervals, e.g. re-authenticating with the system every 5 minutes. Note that this however implies a higher network traffic load at the AAA server, potentially affecting the scalability of our solution in a negative way.

5 Results and Conclusion

As presented in [1], our system for multimedia sharing is based on existing operator infrastructure, e.g. HGWs and AAA server that is already deployed or that will have to be deployed for FMC. Further we enabled a very large group of compatible equipment (end user devices, media servers, AAA servers) by choosing to rely on standard mechanisms such as UPnP, HTTP and RADIUS. Since we proposed to reuse critical operator infrastructure we had to ensure that our system does not overload or endanger said infrastructure. Consequently we discussed scalability, fault tolerance and security aspects of our system in this article in details:

We showed that our proposed system scales well as it requires little overhead for AAA communication and media itself is exchanged in a peer to peer approach directly between the involved home networks.

It is worthwhile noting that our system relies on the operator's AAA infrastructure as its linchpin. Since operators ensure the fault tolerance and scalability of the AAA server, we consider this to be beneficial for the fault tolerance of our solution – all other components that fail will only affect the directly associated users, not endangering the system functionality as a whole.

We also showed which methods our prototype implementation uses to prevent unauthorized access of media. Security considerations were presented for the steps of Authentication of the visiting mobile device, Service Access and Service Termination. Furthermore, we listed possible measures to further enhance security of the overall system such as user or filename based access control lists or encrypting the media exchange between the home networks.

Acknowledgments

This work has partially been supported by the Nordic Interaction and Mobility Research Platform (NIMO) project [24] funded by the InterReg IVA North program.

References

[1] R. Ul Islam, M. Schmidt, H.-J. Kolbe, and K. Andersson, "Nomadic Mobility between Smart Homes," in *Proc. of 2012 IEEE Globecom 2012 Workshops (GC Wkshps'12), Anaheim, California, USA*. IEEE, December 2012, pp. 1062–1067.

[2] C.-L. Wu, C.-F. Liao, and L.-C. Fu, "Service-Oriented Smart-Home Architecture Based on OSGi and Mobile-Agent Technology," *IEEE Transactions On Systems, Man, and Cybernetcis—Part C: Applications and Reviews*, vol. 37, no. 2, pp. 193–205, March 2007.

[3] "OSGi Alliance," http://www.osgi.org, August 2014. [Online]. Available: http://www.osgi.org

[4] M. Kwan, "OSGi-Based Smart Home Architecture for Heterogeneous Network," in *Proc. of the 3rd International Conference on Sensing Technology (ICST'08), Tainan, Taiwan*. IEEE, November 2008, pp. 527–532.

[5] D. Granlund and C. Åhlund, "A scalability Study of AAA Support in Heterogeneous Networking Environments with Global Roaming Support," in *Proc. of the IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'11), Changsha, China*. IEEE, November 2011, pp. 488–493.

[6] B. Hirsch, T. Konnerth, A. Heler, and S. Albayrak, "A Serviceware Framework for Designing Ambient Services," in *Proc. of the 1st International Conference on Ambient Intelligence Developments (AmID'06), Sophia-Antipolis, France*. Springer Paris, September 2006.

[7] Z. Fan, B. Yin and S. Zhang, "A Mobile Service Middleware supported 4G Adaptive Multimedia Applications," in *Proc. of the 7th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), Taipei, Taiwan*. IEEE, December 2006, pp. 352–357.

[8] L. Brewka, P. Sköldström, A. Gavler, V. Nordell, H. Wessing, and L. Dittmann, "QoS Enabled Resource Allocation over an UPnP-QoS - GMPLS Controlled Edge," in *Proc. of the 2011 IEEE Consumer Communications and Networking Conference (CCNC'11), Las Vegas, Nevada, USA*. IEEE, January 2011, pp. 218–222.

[9] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2865, June 2000.

[10] "UPnP Forum," http://www.upnp.org, August 2014. [Online]. Available: http://www.upnp.org

[11] P. Calhoun, M. Montemurro, and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Specification," IETF RFC 5415, March 2009.

[12] P. Calhoun, M. Montemurro, and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11," IETF RFC 5416, March 2009.

[13] "3GPP and Broadband Forum," http://www.3gpp.org/3GPP-and-the-Broadband-Forum, August 2014. [Online]. Available: "http://www.3gpp.org/3GPP-and-the-Broadband-Forum"

[14] B. F. TR-203, *Interworking between Next Generation Fixed and 3GPP Wireless Networks*. Broadband Forum, August 2012.

[15] B. Aboba and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)," IETF RFC 3579, September 2003.

[16] 3GPP, *TS 23.234, version 11.0.0: 3GPP System to Wireless Local Area Network (WLAN) Interworking; System description*. 3GPP, September 2012.

[17] ——, *TS 24.327, version 11.0.0: Mobility between 3GPP Wireless Local Area Network (WLAN) Interworking (I-WLAN) and 3GPP systems; General Packet Radio System (GPRS) and 3GPP I-WLAN Aspects; Stage 3*. 3GPP, March 2012.

[18] ——, *TS 33.234, version 11.4.0: 3G Security; Wireless Local Area Network (WLAN) Interworking Security*. 3GPP, June 2012.

[19] "Home Gateway Initiative: HGI remote access," http://www.homegatewayinitiative.org/publish/HGIremoteaccessv1.01.pdf, May 2008. [Online]. Available: http://www.homegatewayinitiative.org/publish/HGIremoteaccessv1.01.pdf

[20] "ETSI TISPAN," http://www.etsi.org/tispan, August 2014. [Online]. Available: http://www.etsi.org/tispan

[21] "AdvOSS," http://www.advoss.com, August 2014. [Online]. Available: http://www.advoss.com

[22] "FreeRadius," http://freeradius.org, August 2014. [Online]. Available: http://freeradius.org

[23] IEEE, *IEEE 802.1x-2010, Port Based Network Access Control, IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control*. IEEE, February 2010.

[24] "NIMO: Nordic Interaction and Mobility Research Platform," http://www.nimoproject.org, August 2014. [Online]. Available: http://www.nimoproject.org

Author Biography

Raihan Ul Islam is a Ph.D. candidate at Technical University of Darmstadt (Telecooperation Group). His main research focus is on Quality of information for Dynamic Data Storage. He received his M.Sc. degree in Computer Science from Luleå University of Technology, Luleå, Sweden. Previously he worked as a software engineer at NEC Laboratories Europe, in the Context-aware Services (CAS) and Smart Environments Technologies Group. His research interests also include Machine Learning, M2M Communication, Smart Home and City, Mobile Systems, Pervasive and Ubiquitous Computing.

Mischa Schmidt is a Senior Researcher at NEC Laboratories Europe, working in the Smart Grid Services Platform Group. He received his diploma degree in computer science with special focus on Computer Vision, Computer Graphics and Pattern Recognition from the University of Mannheim, Germany in 2003. He was active in the Standardization of Next Generation Telecommunication Networks in IETF and in ETSI TISPAN where he was vice-chair of WG3 (protocols) and Rapporteur of multiple standards. His current research interests include M2M communication, data analysis and machine learning in the context of energy management.

Hans-Joerg Kolbe holds a Ph.D. in Physics from University of Marburg and leads the Software Defined Networks Group at NEC Laboratories Europe in Heidelberg. His group's research, standardization and sales support areas include software-defined networking, network functions virtualization, network management and information-centric networking. Prior to joining NEC in 2007, he was responsible for the broadband network design at Arcor AG & Co KG, which later became part of Vodafone. In addition to leading R&D and marketing activities, Hans-Jörg is heading NEC's delegation at the Broadband Forum.

Karl Andersson received his M.Sc. degree in computer science and technology from Royal Institute of Technology, Stockholm, Sweden, in 1993. After spending more than 10 years as an IT consultant working mainly with telecom clients he returned to academia and earned his Ph.D. degree from Luleå University of Technology (LTU) in 2010 in Mobile Systems. Following his Ph.D. degree and a postdoctoral stay at Internet Real-Time Laboratory, Columbia University, New York, USA, Karl was appointed Senior Lecturer and Associate Professor of Pervasive and Mobile Computing at LTU in 2011 and 2014 respectively. During Fall 2013 he was also a JSPS Fellow at National Institute of Information and Communications Technology, Tokyo, Japan. His research interests are centered around mobility management in heterogeneous networking environments, mobile e-services, and location-based services. Karl is a senior member of the IEEE and a member of ACM.