

# Mobile Device Connectivity in Home Networks

Mika Saaranen<sup>1</sup>, *Member, IEEE* and Dimitris Kalofonos<sup>2</sup>, *Member, IEEE*

**Abstract**—A number of technologies are emerging that enable the creation of a market for networked consumer electronic devices for home use. As this market emerges, the research area of home networking is increasing in importance. In this paper, we first present some motivating use cases from the application area of networked home entertainment to illustrate the requirements posed on home networks, both for local and for remote access. The emphasis is on the use of mobile devices. We describe the challenges facing both the manufacturers and consumers in creating and using such home networks. Since the users of these systems are non-expert consumers, we argue that the most important challenge is creating easy-to-use, self-configuring and self-healing home networks. Finally, we present a de-centralized architecture and an overview of technologies that can be used to enable local and remote access to home networks using mobile devices.

**Index Terms**—Home networking, networked consumer electronics, local home access, remote home access.

## I. INTRODUCTION

Networking at home has traditionally meant connecting home PCs to the Internet through a modem line or a broadband connection. Local networks such as Ethernet have been very rare in the home environment. Home networking has its roots in building automation applications, with technologies like LonMark [1] or X.10 [2], but these have not been widely used in private homes, although many new buildings do incorporate this kind of technologies. This traditional image is now being changed with the emergence of digital media consumed natively on various home devices and with the current boost on Wireless Local Area Networks (WLAN) at home and in public places.

Despite the focus being on providing connectivity over wide area networks, the Internet community has defined and deployed almost all necessary technology components needed for home networking and consuming media. For instance, TCP/IP, HTTP, RTP have been defined in IETF and deployed also on other networks like GPRS or UMTS. In addition, media formats like JPEG and MPEG1 layer 3 (more commonly known as MP3) are widely adopted by the Internet community.

When these technologies are combined with WLANs and Ethernet, we have the seeds of an emerging new era of home networking. From the manufacturers’ point of view, this Internet-technology-based home networking appears appealing because it enables new product concepts. First, completely new kind of devices for home media consumption and storage can be made, such as media servers that can store hundreds of hours of movies. On the other hand, digital content can be stored and served from home PCs after it has been downloaded from the Internet, as some already existing products demonstrate. Second, networked devices may exclude local user interface allowing both for smaller devices and, especially, for lowering the manufacturing cost of the devices. In this scenario, a networked remote controller, possibly provided by a different vendor, would provide the user interface. Also, common networking technologies promise a reduction on the amount of distinct wiring necessary, thus making home networking more feasible for consumers. Remote control of home media devices may also extend to mobile terminals capable of Internet connectivity, even if they are used in remote locations.

When consumers start deploying networked home appliances, usability and ensured interoperability between home appliances is of prime importance. Although usability is mostly based on manufacturers’ ability of designing good products, the ensured interoperability requires standardization or industry approved guidelines. There have been many efforts in standardizing a home architecture, such as the Home Audio Video interoperability (HAVi) [3] and the Digital Living Network alliance (DLNA) [4]. For instance, these two forums define a complete set of technologies providing all pieces from communication to applications and from zero-configuration to advanced control of home devices. These forums have applied different approaches to the architecture, making their approaches more or less applicable to different audiences.

In this paper we focus on home networking including local and remote connectivity. We briefly review related work on home connectivity and some of the most interesting basic use cases. We discuss the challenges that face both users and manufacturers. We argue that the most important challenges are on usability and automatic configuration of the home network and its devices. We also present a home networking architecture based on Internet and IEEE 802 technologies and a review of many alternative connectivity methods. We also discuss remote connectivity and present two potential

<sup>1</sup> Mika J. Saaranen is with Nokia Technology Platforms, Tampere, Finland. E-mail him at [mika.saaranen@nokia.com](mailto:mika.saaranen@nokia.com).

<sup>2</sup> Dimitris N. Kalofonos is with the Pervasive Computing Group, Nokia Research Center, Boston, MA. E-mail him at [dimitris.kalofonos@nokia.com](mailto:dimitris.kalofonos@nokia.com).

technologies for mobile devices accessing home appliances remotely.

The remaining of this paper is organized as follows: Section II presents a brief overview of related work; Section III introduces some basic use cases for home connectivity and Section IV introduces the challenges of building solutions for home networking. Section V introduces an architecture and potential technologies for local and remote home connectivity. Finally, the conclusions of this work are discussed in Section VI.

## II. RELATED WORK

Related work on this area can roughly be divided into two areas: standardization and academic research. Furthermore, there are many exciting products emerging in the industry, but in this paper we will not refer to commercial product efforts. The two first standardization forums presented here (HAVi and DLNA) have defined a de-centralized home network that is mainly targeted for home entertainment applications.

The HaVi [3] approach to home networking is based on IEEE 1394 that provides high data rates with guaranteed QoS. HAVi defines full architecture with hot plug-and-play-features. Device architecture allows installing Java based SW modules for the provision of device control. HAVi provides non-IP networking, but facilitates gateway solutions that allow Internet connectivity.

DLNA [4] has taken an alternative approach, basing its technology choices on protocols and formats used mainly in the Internet community. Device discovery and control is based on Universal-Plug-and-Play (UPnP) [5]. DLNA aims at creating interoperability guidelines based on existing standards, rather than defining new technologies. The goal is to instruct device manufacturer’s to use DLNA defined technologies in an interoperable way. In this paper we will present an architecture that is compatible with this DLNA approach.

An alternative approach, which can be characterized as centralized, has been taken by the Open Services Gateway Initiative (OSGi) [6]. OSGi is a versatile framework that provides APIs and Java execution environment for building integrated home networks and adaptation functions between various other solutions like UPnP controlled devices. In this approach, various networking and service provision environments are connected through services that the OSGi gateway provides. If the OSGi gateway and its services are well implemented, it may provide valuable additional services, without invalidating existing networked services.

In academic research literature, most advanced solutions are part of the Pervasive Computing area of research. Advanced solutions are proposed, including determining the location or intent of the people and acting based on observed behaviors. Well known example in this area is Project Aura from CMU [7]. The work in [8] presents a proposal that provides a ubiquitous computing environment with location-based services at home. The implementation uses mainly standard protocols such as SLP [9] and SIP [10] for controlling and discovering home appliances.

Another direction of research focuses on building middleware solutions that aim to solve problems, such as zero-configuration, usability and interconnecting non-compatible technologies together. In [11] the authors present a unified home services interface, behind which real devices are hidden and meta-devices that can combine several individual devices. An OSGi-based home architecture is presented in [12].

## III. BASIC HOME USE CASES

In this paper we focus on home entertainment-related use cases and on the local and remote access connectivity issues related to these use cases. In the rest of this section we present four main use cases, from which more detailed use cases could be derived.

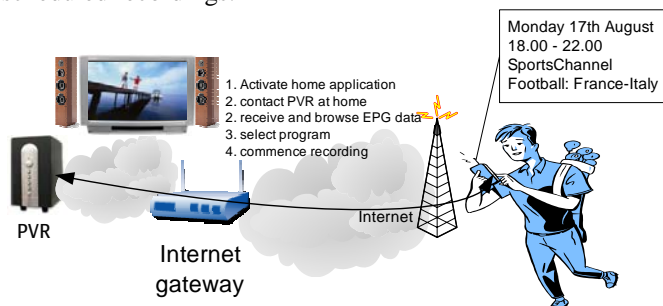
Maybe the most frequent use case in the home environment is to consume media content from local or external source. Media content can be, for instance, your favorite TV show or listening CDs or MP3s. Figure 1 shows a typical case where a user is watching a prerecorded movie from a media server. In this case, the user will activate the TV set and the media server, browse and select the desired movie and start up playing the movie at the selected TV set. The media server can be e.g. a media PC, a DVD player or a set top box. After watching the movie, the user may select a new program or turn off the devices. This scheme is also valid for listening radio or CDs or MP3s from a stereo equipment.



**Figure 1: Use case for locally watching a movie.**

Related to the previous case, in many cases people desire to record broadcasted programs for later consumption, e.g. when the weekly transmission of some program happens on an inconvenient time. Actual programming is usually done while in close proximity of the recording device, but the remote access case shown in Figure 2 is also interesting, as mobile life style is getting more popular. The basic use scenario, either in the remote or the local programming case, would be first activating the remote controller. In the local case this may just mean picking the remote controller, but in the remote case the user would have to start a home access application and potentially accept usage of a cellular or public WLAN

network. The next phase would be finding out when and in which channel the desired program shall run. In an advanced scenario, the home recording device would show program information from an Electronic Programming Guide (EPG) and the user could just select the program. However, the current way of operation, i.e. just entering the starting and ending times and the channel numbers, is expected to remain as a backup method. After the programming has been completed, the user may also want to see the list of his/her scheduled recordings.



**Figure 2: Use case for remote PVR programming.**

In the current MP3 player boom, managing and synchronizing a music collection will have significant role. In particular, smaller music players may store only a fraction of the whole music collection, therefore creating the need to update the collection while inside or outside the home. As WLAN connectivity will provide almost free access, such a mobile update will be feasible also at a reasonable cost.

Currently, sharing of multimedia content is getting more and more popular. This would be the fourth type of use case, where sharing media content between friends will have a significant role. In relation to home usage, the typical scenario would be exchanging selected songs with your friends visiting your home. This sharing presents legal challenges because the copyrights of the content owners should be protected, but in the same time legal sharing should not be limited.

There are many alternative use cases that can be derived from the examples we described and also totally unrelated to these. Currently, the digital networked home is taking its first steps and therefore new ways of exploiting this technology will emerge in the future.

#### IV. HOME NETWORKING CHALLENGES

There are a number of technical challenges that have to be addressed in order for home networks to be deployed successfully and be in a position to enable this multitude of new use cases. The main difference between home networks and traditional networks in the corporate world, is that the persons setting up and maintaining them are everyday consumers, with little or no knowledge of networking technologies. Also, the deployment of these home networks is happening in a completely decentralized way, without coordination among the consumers located in the same area, in contrast to professionally installed networks where there is a significant effort in planning prior to deployment potentially

interfering networks. The above factors, combined with the market pressure to minimize the cost of home networking products, create some unique challenges in research aiming at home networking.

In general, it is expected that home networks will be set up and managed by everyday consumers and not by trained professionals. Therefore, the networking technologies employed must enable home networks to be **self-configurable** as much as possible, with minimal or no intervention from the consumers themselves. The required approach puts the burden on product and protocol design rather than network administrators, as opposed to the traditional approach in networking. The home network architecture should include auto-configuration protocols (e.g. [13], [14]) that will enable a “buy-plug-and-play” experience for consumers. Besides the required protocols, the product designs should provide a user interface which should hide the technical network complexity from the users as much as possible and interact with them only through intuitive mechanisms, e.g. through interactive “wizards”, real-world intuitions such as “touch” and “point-and-click”. The home network architecture should support incremental network deployment, enabling the easy and seamless integration of new network nodes as consumers buy and bring home new products. Finally, the product design should enable non-experts to easily make administrative changes to existing home networks to accommodate new users, new services and new usages of home devices.

Besides the challenge of enabling self-configuring home networks that are appropriate to be set up and maintained by non-expert consumers, it is equally important that the home networks are designed to be as **self-healing** as possible. Since home networks are deployed by non-experts, with little or no planning and no coordination with other consumers, it is very probable that they will be prone to erratic behavior. Examples of problems that may be encountered are radio interference and crosstalk, inadequate bandwidth, excessive round-trip delays, network congestion, addressing conflicts, uneven wireless coverage, inappropriate timer time-outs, as well as a range of other problems. The consumers would be unable to pinpoint the source of all these problems and are likely to attribute the problems to the home products themselves. This can lead to a very frustrating user experience and bad marketing perception for the manufacturers of home devices. Creating self-healing home networks requires both new protocols and middleware, as well as an approach to product and application design which anticipates erratic network behavior and handles it gracefully. For example, disconnections should not stall node resources and require rebooting by users, but rather products should be designed to auto-resume where possible or exit gracefully by providing easy-to-understand error explanations to users. Finally, manufacturers would have to develop new network monitoring and debugging tools, which would be easy-to-use by non-expert consumers and would suggest to them potential fixes whenever problems occur. Alternatively, new tools and services would have to be provided by 3<sup>rd</sup>-party technical

support companies under contract by the consumers, which will monitor, detect and correct home network problems remotely, with minimal or no intervention by the consumers themselves.

Another important challenge in the design of home-networks is **security**. Many of the component networking technologies (e.g. 802.11 [15], HomePlug [16], cellular networks for remote access) are based on sharing a transmission medium which is accessible by many other users. This creates a potential vulnerability for home networks which may be exploited by malicious users with a devastating effect on the usability of the home networks. In a professionally administered private network environment, administrators take several countermeasures to thwart attacks and allow only authorized access to the nodes and services in the private network. However, such sophistication cannot be assumed in a home network environment. The home architecture should include enough security mechanisms at the link-level (e.g. WEP [15], WPA [17], 802.1X [18], 802.11i [19], Bluetooth Security [20]), network-level (e.g. IPsec [21]), transport-level (e.g. TLS [22], HTTPS [23]) and application level (e.g. UPnP Security [24]). Equally importantly, the applications and products should be designed in a way to allow easy configuration of security because otherwise consumers will not use it. The example of the proliferation of 802.11-based home networks, many of which are even now used without security enabled, gives a colorful illustration of the magnitude of this problem. Finally, as in the case of regular network problems, new tools and services would have to be developed that would detect and address the inevitable malicious attacks in home networks. Again this should happen with minimal or no intervention by the consumers themselves and could be performed by 3<sup>rd</sup>-party companies under contract.

Remote access to home networks is also expected to present a range of serious challenges both to product designers and to consumers themselves. The users would like to access the devices and services of their home networks remotely, while enjoying an experience as close as possible to that of being physically located at home. However, the location and method of remote network attachment can create vastly different connection characteristics when accessing the home remotely. Example of characteristics that vary widely include the bandwidth and round-trip delay (e.g. GPRS vs. DSL vs. 802.11), cost (e.g. cellular vs. 802.11), security requirements (e.g. access from a corporate intranet vs. access from a Café WLAN hot-spot) and capabilities of the devices used for remote access (e.g. desktop vs. laptop vs. mobile phone). It is an important challenge to design systems and products that create a user experience as uniform as possible and that allow the user to select the best available remote access method best on his/her desired task (e.g. remote recording programming vs. content streaming), context (e.g. location) and preferences (e.g. connection cost profile). Finally, other challenges related to remote access include the use of dynamic IP addresses in typical broadband connections, as well as traversing firewalls and NATs that effectively prevent outside connectivity.

Finally, mobile devices face particular challenges when connecting to home networks. Specifically, mobile devices face more frequent disconnections as users move in and out of range of local Access Points and experience signal fading or interference when users roam while remotely accessing their home networks. Also, mobile devices have limited resources such as computational power, battery life and screen size, all of which pose extra networking requirements when accessing the home networks locally or remotely. Finally, it is mobile devices that are most commonly used when visiting other home networks. Enabling the “visitor scenario” poses more challenges both for users and manufacturers, both from the home network architecture and system design perspective, as well as from the perspective of usability and ease-of-use.

## V. LOCAL AND REMOTE HOME CONNECTIVITY: ARCHITECTURE AND TECHNOLOGIES

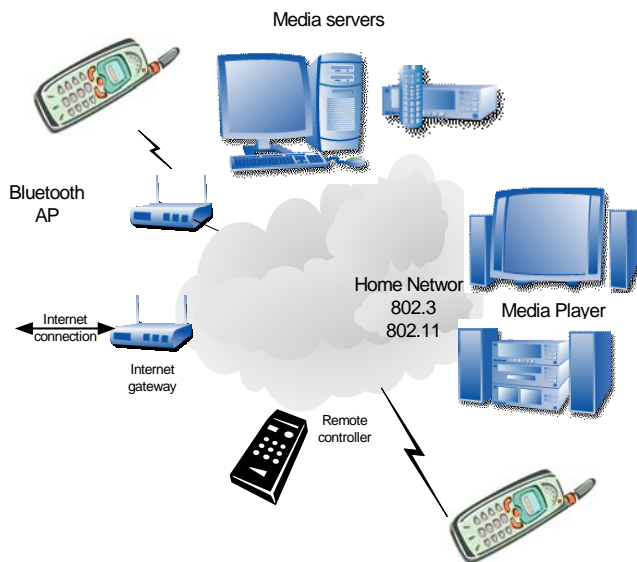
### A. Overview of Home Connectivity Architecture

As mentioned earlier, there are many alternatives for the home networking architecture. While many options suggest using a centralized architecture that provides a unified service framework, the trend seems to be moving towards a de-centralized approach built on IEEE 802 LAN protocol-family and Internet-based technologies. As already mentioned, the DLNA is an example of this kind of approach allowing home networks to be built gradually based on individual needs. Also, as these technologies are mostly mainstream implementations, the migration costs can be minimized. In the de-centralized model, automatic configuration and ease-of-use features cannot rely on a central element to hide the various technologies behind uniform APIs and middleware. Therefore, service discovery protocols are used to provide a similar way of creating methods for discovering and controlling home devices. Also, in this approach application protocols and media formats must be agreed upon carefully and special attention must be given to usability and auto-configuration features.

This de-centralized home architecture is based on a layered approach. At the lower-level, the home connectivity relies on widely used TCP/IP networking technologies, which are built on top of a variety of link-level bearers and topologies. At the middle-level, TCP/IP-based device discovery and control technologies such as UPnP [5], SLP [9] are used to enable a distributed computing environment. Finally, at the higher-level of the architecture are the applications and the media formats that ensure interoperability and usability of the system.

### B. Local Connectivity

As mentioned earlier, the architecture model presented here for home networks is based on the de-centralized approach, similar to that chosen in DLNA interoperability guidelines [4]. An example illustration of this architecture model for local network connectivity is depicted in Figure 3.



**Figure 3: Overview of local access architecture.**

The general de-centralized model for local connectivity allows the organization of networks of home devices in two different modes: infrastructure-based and ad-hoc (or peer-to-peer) based. In the case of infrastructure-based node organization, network elements such as Access Points (AP), switches, routers, DHCP servers, etc. are used to create one or more subnets comprising of fixed and mobile home devices, which are all connected with each-other through a semi-static network configuration and topology. The infrastructure-based approach requires dedicated nodes to provide network-level services and usually some implicit or explicit network configuration by the users. In the case of ad-hoc-based node organization, a subset of home devices connect and communicate with each other opportunistically, whenever user or application actions require it, usually for a short period of time, after which these ad-hoc networks dissolve. A common example of this organization mode is point-to-point interactions between two devices, for example when showing pictures taken with a Bluetooth-enabled mobile phone on a Bluetooth-enabled TV set. Both the infrastructure-based and the ad-hoc-based modes must present the same network abstraction to higher-level layers (i.e. create an IP layer), to enable applications to operate seamlessly regardless of the link-level network configuration mode. Some link-level technologies enable easier interaction in an infrastructure configuration (e.g. 802.11 [15]), while others provide special features to enable easy ad-hoc interactions (e.g. Bluetooth [25], [26]). It is expected that home networks will feature a combination of both the infrastructure and ad-hoc modes of node organization.

In the same way that the link-level topologies can vary widely, the link-level bearers may also be very different, as long as they present a network abstraction layer based on IP to higher-layer protocols. Of course, the inherent characteristics of the different link-level technologies have a significant impact on the perceived Quality of Service (QoS) of the IP connection (e.g. bandwidth, delay, delay variation) by the applications. Therefore, different bearers are suitable to

support different types of applications, depending on their QoS requirements. Overall, the issue of QoS support in a home network is a challenging one. Home networks will probably be composed by a multitude of link-level technologies, most of which do not offer QoS guarantees. Therefore, a priority-based QoS mechanism (e.g. [27], [28]) seems more applicable than reservation-based QoS mechanisms in home networks.

Some of the most important link-level technologies for local connectivity in home networks are the following:

- 802.3 (Ethernet 10/100/1000 Mbps) [29]: Ethernet has been the most common link-level technology in traditional IP-based Local Area Networks (LAN). It is a well established technology which offers high data-rates (e.g. Gigabit Ethernet), low delays and high-reliability. It is more suitable for fixed home devices as it restrains mobility; however, it can be used to connect mobile devices when the users are not moving (e.g. an Ethernet cradle/charger for a digital camera). The most serious issue for its wide adoption in home networks is that it requires cabling the home, which is not always feasible. It is expected, however, that most new home constructions in the future will support high-speed Ethernet cabling in the same way they offer telephone wiring today.
- 802.11 a/b/g (Wi-Fi) [15], [30], [31], [32], [33]: 802.11 is without a doubt the most successful wireless local access technology today. It is one of the big enablers of home networks, as it is an inexpensive technology which can be used to instantly connect home devices scattered around the home, without the need for any costly cabling. It also offers relatively high data-rates (order of 10s of Mbps), allows for mobility within the home and it is suitable for laptop PCs and mobile devices. 802.11 provides seamless support for Ethernet and IP. As with all wireless technologies operating in the unlicensed spectrum, 802.11 is vulnerable to interference from other wireless networks, a problem which is expected to intensify because of the commercial success of this technology. Issues with interference and signal fluctuation may lead to a negative user experience in some applications (e.g. streaming video with strict high-bandwidth, low-delay requirements). Finally, since all wireless technologies operate over a shared medium, appropriate security measures have to be taken to prevent unauthorized use of 802.11-based home networks.
- Bluetooth [25], [26]: Bluetooth is a short-range wireless technology, popular mainly in mobile phones and other mobile devices because it combines low power consumption, low cost and ad-hoc networking features. Bluetooth was created as a cable-replacement technology and this still remains its main usage today. Bluetooth specifies support for Ethernet encapsulation with the Bluetooth Network Encapsulation Protocol (BNEP) [34] and support for IP as specified in the Personal Area Networking (PAN) [35] profile. Bluetooth offers relatively low data-rates (order of 1-3

Mbps) and is not very suitable for connecting a large number of devices. Although Bluetooth Access Points can be used to provide local connectivity in the infrastructure mode of node organization mentioned above, it is more likely that it will be mainly used in the ad-hoc mode of organization for point-to-point interactions.

- UltraWideBand-UWB (WiMedia) [36], [37]: UWB is an emerging wireless technology for short-range, high-speed communication. It is described as a technology offering high bandwidth (order of 100s of Mbps) and low power consumption, which makes it a good match for power-constrained mobile devices with rich multimedia capabilities. It is possible that UWB will replace Bluetooth in devices where higher data rates are required. Recently the Bluetooth SIG announced that it intends to explore the convergence of Bluetooth and UWB technologies. Also, the USB Forum announced the availability of the Wireless USB specification, based on WiMedia UWB technology [38]. The main issues that may delay the wide deployment of UWB in home networks are lack of broad consensus in UWB standardization and regulatory obstacles in some regions outside the US.
- IEEE 802.15.4 (Zigbee) [39]: Zigbee is a wireless technology for local access designed to offer low data-rates (order of 100s of Kbps) and very low power consumption. It offers seamless support for Ethernet and IP and is suitable for connecting a large number of devices. Its characteristics make it a strong candidate for home automation applications involving sensors and actuators, where nodes only need to transmit low data-rate streams but have high requirements for conserving power.
- HomePlug [16]: HomePlug is a wireline technology that supports Ethernet over existing electrical power wires at home. HomePlug adaptors can be plugged in regular electrical power sockets, thus easily creating Ethernet LAN segments connecting all devices scattered around the home. HomePlug technology supports high data-rates (order of 10s of Mbps) and can be suitable for transmission of multimedia content. Obviously, the biggest appeal of this technology is that it uses wiring which is available in all current and future homes. Since the power grid often has wiring segments shared by multiple homes, security threats can be considered similar to the case of 802.11. On the negative side, sometimes not all rooms in a home are connected by the same power wiring, which prevents the technology from creating fully connected home networks. Also, often power wiring has poor signal propagation properties and suffers from cross-talk, which may have a negative impact on the perceived user experience.
- IEEE 1394 (FireWire) [40]: FireWire is a serial bus wireline technology, which was originally developed to provide a high-speed serial connection between devices. It supports very high data-rates (order of 100s

of Mbps) and a synchronous mode of operation which can guarantee bandwidth to devices. The technology is suitable for connecting several devices at the same time and extensions have been proposed to support Ethernet and IP traffic. However, currently it is still mainly used for point-to-point interactions. Also, it is possible that FireWire technology may come under pressure from the ubiquitous and cheaper alternative of USB 2.0 which offers similar data-rates.

- Near-Field Communications (NFC) [41]: NFC is a very close proximity wireless technology, which can be used for two-way communication between two devices. Since NFC communication occurs only if the two devices practically "touch" each other, it offers a new, intuitive and inherently secure user interaction modality. NFC is a technology that grows in importance and it is expected that it will be incorporated in many mobile devices in the future. NFC itself is suitable for IP traffic exchange, but its significance in home networking can be even bigger as an out-band mechanism used for intuitive initialization of some other in-band bearer, to be used to carry the actual IP traffic.
- Other technologies that may play some role in home networking include USB [38] and HomePNA [42].

Mobile devices can use any of the above wireless or wireline link-level bearers to connect locally with other devices in the home network. Of course, wireless bearers are much more common because they enable users to move freely while using their mobile devices. Comparing to fixed home devices connected through wireline bearers, mobile devices using wireless bearers have two important additional problems to overcome: limited power resources and unreliable connections to the home network:

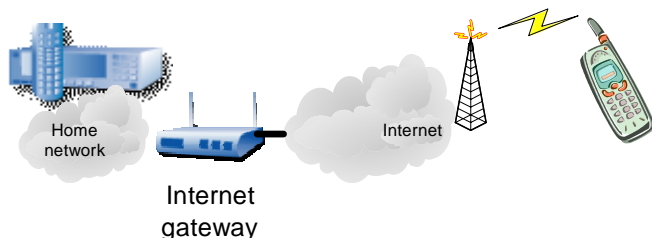
- To reduce power and conserve energy, wireless bearers define low-power modes of operation. In general, the higher the power savings of these modes, the lower the effective throughput and the higher the delay experienced by the mobile devices. In some cases, when a very low power mode is entered, the device appears temporarily disconnected from the home network. To optimize energy conservation while maintaining full functionality, often mobile devices must be aided by proxies in the network, which perform certain functionality on their behalf while they are unavailable because they are saving power. Also, it is important that traffic filtering takes place (e.g. at the Access Point) so that only necessary traffic reaches the mobile devices, to allow them to enter the low-power modes for as much time as possible.
- To deal with frequent disconnections caused by signal fluctuations, interference and user mobility, it is important that home applications running on mobile devices are designed in a way that tolerates poor network connectivity. In addition, there are proposals for specialized middleware (e.g. [43], [44]) that can provide the necessary end-to-end session support against

disconnections and network interface changes (horizontal or vertical mobility), transparently to home applications.

### C. Remote Connectivity

Until recently, the home has been mostly considered as an isolated network environment, where the only outside connectivity has been Internet access from home PCs. Earlier remote access to the home had to be implemented over telephone lines, making it expensive to use and providing only narrow-band connectivity.

Currently, mobile terminals like phones are mostly capable of Internet connectivity and also a significant portion of homes have broadband Internet connection. This creates a connectivity enabler that provides low-cost access with sufficient data rates for many applications. There are, however, challenges on reaching the home network from a remote location. First, typical broadband connections use dynamic IP addresses that in many cases are not even public. Second challenge is firewalls and NAT boxes that effectively may prevent outside connectivity. There are potential solutions, e.g. paying extra for fixed public IP address, but in this paper we do not address this part of the problem.



**Figure 4: Overview of remote access architecture.**

Figure 4 shows a high level architecture for remote access to the home using a mobile device. The mobile terminal is connected to the Internet through either a cellular network or through some local WLAN Access Point (e.g. 802.11). Today, from the point of view of cost and bandwidth, WLAN access would be preferable for transferring large amounts of content, while cellular access would be more reasonable for transferring single songs or schedule recordings. However, the cellular costs are dropping and available bandwidth is increasing, so in the future full synchronization over cellular networks will be very feasible.

There are several ways to implement actual remote access. One option would be using a 3<sup>rd</sup>-party service (e.g. [45]) that allows accessing from a remote location home media content that resides in a home PC. In this paper, however, we will focus on two connectivity solutions, a proxy solution and a VPN-based solution, which involve only an Internet gateway at the edge of the home network and not some 3<sup>rd</sup>-party server somewhere else in the Internet.

In the proxy solution, there is a home proxy located at the Internet gateway device. Inside of the home the proxy uses e.g. UPnP to discover and control home devices. At the proxy, this information and potential control actions are converted into some form of HTML pages. The proxy is seen as a web

server by the mobile terminal which accesses the home services from a remote location. All actions that the mobile terminal accesses from the HTML pages are converted into corresponding UPnP actions and vice versa. In this solution, any web browser can be used for remote access allowing in practice any terminal to be used. Also, authentication and authorization mechanisms are well known and HTTP traffic is typically able to traverse firewalls. Well-known encryption protocols e.g. TLS/SSL can be used to provide adequate level of security. On the other hand, the proxy solution may provide inefficient control of devices and limits the user interface and actions that can be performed remotely only to methods that can be supported by web browsers.

An alternative solution could be provided based on Virtual Private Networks (VPN) technologies [46]. VPN creates a protected tunnel between the mobile terminal and the home network using e.g. IPSEC [21]. There is a need for a VPN gateway at the Internet gateway and also a VPN client at the remote terminal. In this scenario, the terminal can contact the home devices much like being locally present in the home network, except with increased delay and lower data rates. Although it is possible to use local service discovery protocols over VPN, this may not be the optimum solution for maintaining the status of the network. For instance, UPnP maintains the status of available services by sending advertisements and discovery messages that are multicast to all devices. Although for local networks these periodic and repeated messages may not be a considerable burden, they may cause a significant load for VPN tunnels over remote networks. Therefore, there is a clear need for solutions that allow preventing unnecessary signaling to enter the VPN tunnel, but at the same time provide adequate information for the remote terminal to access the home services. The UPnP forum [47] is currently working on this problem domain to provide more appropriate solutions for remote access. The VPN-based solution for remote access requires that a VPN gateway service is available at home and its configuration is not an easy task for the ordinary consumer. On the other hand, the VPN-based solution allows the terminal to use exactly the same applications and user interfaces that can be used when accessing the home network locally. From the user point of view, this makes remote access of home services easier to use.

Regardless of the chosen approach, usability and security remain vital issues for any remote access products. In both approaches, the actual use of home services can be pretty easy, but the initial set-up of the VPN gateway or the home proxy must be extremely easy. The main responsibility will remain with the device vendors to create e.g. easy-to-setup wizards; however, innovative ways of transmitting e.g. security and network settings from the new devices are required. One alternative would be that ISPs would provide a remote access service as an additional service for their broadband access service.

Remote access to home is an important service in the mobile life that we are living. All approaches presented earlier can co-exist and in the future we shall see more advanced

services that will bring additional value for the consumers.

## VI. CONCLUSIONS

In this paper we presented an overview of issues related to home networking, with an emphasis on issues related to mobile devices. We presented some basic use cases for mobile devices to illustrate the requirements posed on home networks, both for local and for remote access. We described the challenges facing both the manufacturers and consumers in creating and using such home networks. Since the users of these systems are non-expert consumers, we believe that the most important challenge is creating technology that makes home networks easy-to-use, self-configuring and self-healing. Finally, we presented a de-centralized architecture and an overview of technologies that can be used to enable local and remote access to home networks using mobile devices. We believe that a de-centralized network architecture that builds on popular link-level bearers (e.g. Ethernet and 802.11) and on widely available Internet-based technologies (e.g. TCP/IP, HTTP) has a high potential of success, because it allows users to build their home networks gradually, while lowering the cost of ownership of such systems as much as possible.

## REFERENCES

- [1] (2005). LonMark International, <http://www.lonmark.org>
- [2] X10 Powerline Carrier Technology, <http://www.x10.com/support/technology1.htm>
- [3] R. Lea, S. Gibbs, A. Dara-Abrams, E. Eytchison, "Networking home entertainment devices with HAVi", Computer Volume 33, Issue 9, Sep 2000, pp. 35 – 43.
- [4] Digital Living Network Alliance (DLNA), "Home Networked Device Interoperability Guidelines v1.0", June 2004.
- [5] UPnP Forum, "UPnP Device Architecture 1.0.1", December 2003.
- [6] P. Dobrev, D. Famolari, C. Kurzke, B. A. Miller, "Device and service discovery in home networks with OSGi", IEEE Communications Magazine, Volume 40, Issue 8, pp. 86-92, Aug. 2002.
- [7] Project Aura home page. <http://www-2.cs.cmu.edu/~aura/>
- [8] H. Schulzrinne, X. Wu, S. Sidiroglou, S. Berger, "Ubiquitous Computing in Home Networks", IEEE Communications Magazine, pp. 128-135, November 2003.
- [9] E. Guttman et al., "Service Location Protocol," v. 2, IETF RFC 2608, June 1999.
- [10] J. Rosenberg et al., "SIP: Session Initiation Protocol," IETF RFC 3261, June 2002.
- [11] P.M. Corcoran, J. Desbonnet, P. Bigioi, I. Lupu, "Home network infrastructure for handheld/wearable appliances", IEEE Transactions on Consumer Electronics, Volume 48, Issue 3, pp.490-495 Aug. 2002.
- [12] X. Li and W. Zhang, "The Design and Implementation of Home Network System Using OSGi Compliant Middleware", IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, May 2004
- [13] S. Cheshire and B. Aboba. Dynamic Configuration of IPv4 Link-local Addresses. IETF Internet draft, Zeroconf, March 2001.
- [14] Droms R., "Dynamic Host Configuration Protocol (DHCP)", IETF RFC 2131, March 1997.
- [15] ANSI/IEEE 802.11, "802.11std. Wireless LAN Medium Access Control and Physical Layer specifications", August 1999.
- [16] HomePlug Powerline Alliance, [www.homeplug.org](http://www.homeplug.org)
- [17] Wi-Fi Alliance, "Wi-Fi Protected Access (WPA)", October 2002.
- [18] IEEE 802.1X, "802.1x-2001 - Port Based Network Access Control", June 2001.
- [19] IEEE 802.11i, "802.11 Amendment 6: Medium Access Control Security Enhancements", July 2004.
- [20] Bluetooth Special Interest Group, "Bluetooth Security Architecture", white paper, version 1.0, 15 July 1999.
- [21] IETF Network Working Group, "RFC2401: Security Architecture for the Internet Protocol", November 1998.
- [22] IETF Network Working Group, "RFC2246: The TLS Protocol, v1.0", January 1999.
- [23] IETF Network Working Group, "RFC2818: HTTP over TLS", May 2000.
- [24] UPnP Forum, "UPnP Security Ceremonies Design Document v1.0", October 3, 2003.
- [25] Bluetooth Special Interest Group, "Bluetooth Core", Specification of the Bluetooth System version 1.1., February 2001.
- [26] Bluetooth Special Interest Group, "Bluetooth Core", Specification of the Bluetooth System version 1.2. , November 2003.
- [27] IEEE 802.1Q, "IEEE standard for local and metropolitan area networks – Common specifications – Virtual Bridged Local Area Networks", May 2003.
- [28] WMM Specification, Wi-Fi WMM (Wireless Multimedia) Specification, Wi-Fi Alliance, March 2004.
- [29] IEEE 802.3, "Local and Metropolitan Area Networks – Specific requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD), Access Method and Physical Layer Specification", March 8, 2002.
- [30] Wi-Fi Alliance, [www.wi-fi.org](http://www.wi-fi.org)
- [31] IEEE 802.11a (Supplement to IEEE 802.11, 1999 Edition), "Local and Metropolitan Area Networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High speed Physical Layer in the 5 GHz Band", Reaffirmed June 12, 2003.
- [32] IEEE 802.11b (Supplement to IEEE 802.11, 1999 Edition), "Local and Metropolitan Area Networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz Band", Reaffirmed June 12, 2003.
- [33] IEEE 802.11g (Supplement to IEEE Std 802.11, 1999 Edition), "Local and Metropolitan Area Networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz Band", June 27, 2003.
- [34] Bluetooth Special Interest Group. Bluetooth Network Encapsulation Protocol (BNEP). February 2003.
- [35] Bluetooth Special Interest Group. Personal Area Networking (PAN) Profile, v1.0. February 2003.
- [36] Wi-Media Alliance, [www.wimedia.org](http://www.wimedia.org)
- [37] Porcino D. "Ultra-Wideband Radio Technology: Potential and Challenges Ahead". IEEE Communications Magazine, July 2003.
- [38] USB Forum, [www.usb.org](http://www.usb.org)
- [39] Zigbee Alliance, [www.zigbee.org](http://www.zigbee.org)
- [40] 1394 Trade Association, [www.1394ta.org](http://www.1394ta.org)
- [41] NFC Forum, [www.nfc-forum.org](http://www.nfc-forum.org)
- [42] HomePNA, [www.homepna.org](http://www.homepna.org)
- [43] V. Zandy, B. Miller, "Reliable Network Connections", ACM MOBICOM'02, September 2002.
- [44] J. Salz, A. Snoeren, H. Balakrishnan, "TESLA: A Transparent, Extensible Session-Layer Architecture for End-to-end Network Services", 4th USENIX Symposium on Internet Technologies and Systems (USITS'03), March 2003.
- [45] ORB networks, <http://www.orb.com>
- [46] C. Metz, "The latest in virtual private networks: part I", IEEE Internet computing," Volume 7, Issue 1, pp. 87-91, Jan.-Feb. 2003.
- [47] UPnP Forum, [www.upnp.org](http://www.upnp.org)