Wireless Residential Network based on IPv6

Timo Kyntäjä
VTT Technical Research Centre of Finland, Espoo, Finland, Europe
timo.kyntaja@vtt.fi

Denis Mischler
Thomson Multimedia, Rennes, France, Europe
mischlerd@thmulti.com

Tom Pfeifer
Fraunhofer Institute for Open Communication Systems (FOKUS), Berlin, Germany, Europe
pfeifer@fokus.fhg.de

Juha Pärkkä
VTT Technical Research Centre of Finland
Tampere, Finland, Europe
juha.parkka@vtt.fi

Abstract

The existing solutions for residential networks have focused on connecting certain types of home appliances to a home network (e.g. A/V devices). The work presented here suggests an IP based resolution for wireless residential network, which is comparable to existing local area networks for public and private organizations. The wireless residential network utilizes heterogeneous wireless technologies and unites the differences with IPv6 and middleware layers.

Keywords

Residential networks, service architecture, WLAN (IEEE-802.11), HiperLAN2, Bluetooth, IPv6

INTRODUCTION

Home as an environment, containing distributed intelligence in numerous devices, has been a topic of discussions and research for a long time. Different residential network products have also been published during the last decade. Hints of future home requirements can be obtained with interviews and prototype tests, but only time will tell for sure which solutions survive and gain user acceptance.

Integration of telecom and Internet creates a possibility to use the services whenever and from wherever needed. This suggests that the services are accessed using different types of terminals, both fixed (e.g. PC, Internet TV) and mobile (e.g. cellular phones, wireless PDAs) terminals. Adaptivity of the service, not only due to the terminal, but also due to the user preferences and use-context are important factors for usability of the service. The aim is towards end-to-end IP based services.

The Future Home project [1] has focused on specifying and implementing a wireless residential networking system. Residential network here contains three different kinds of elements: the network itself with a home server, home appliances, and user terminals. In addition the home network is connected to a remote network, e.g. to Internet.

The main objective of the specified architecture is the integration of heterogeneous wireless technologies, IP version 6, and middleware for services. The aim of the project is to evaluate the specifications and existing technologies to produce clear guidelines for the industry.

In the first chapter the most appealing wireless technologies are presented, depicting the usage for networking at home. The second chapter then presents the system architecture how it can be seen from the viewpoint of IPv6 protocol and its features, the Home Network Service Point (HNSP), the appliances and the terminals. Then the issues related to security, privacy and mobility issues are covered. And finally the main conclusions are presented.

WIRELESS NETWORK TECHNOLOGIES

The Future Home project focuses on three wireless technologies: IEEE-802.11 (WLAN), Bluetooth and HiperLAN2. These have been selected for the following reasons:

- the technologies are complementing from the usage point of view;
- they are in a different phase of maturity and can be also compared against each other;
- these different technologies provide the heterogeneous environment that can be used as a model of a future residential network;
- they all can be used as substitutes of wired connections and therefore are suitable for an IP network environment.

The following sections describe each of these technologies and their residential networking aspects.

WLAN

The IEEE-802.11 standard specifies Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY). The physical layers comprise two versions of radio layers, and an infrared layer. [8]

The radio layers use either Frequency-Hopping spread spectrum (FHSS) or Direct sequence spread spectrum (DSSS) within the 2.4 GHz "Industrial, Scientific, and Medical" (ISM) band, and share the same MAC protocol. They provide for both a 1 Mbit/s and a 2 Mbit/s data payload communication capability.

With the goal of higher bitrates of 6...54 Mbit/s, 802.11a [9] uses the UNII (unlicensed national information structure) 5 GHz band, which is available in the US, but not in Europe or Japan.

Therefore, 802.11b [10] specifies the high rate extension of the PHY for the DSSS system for the 2.4 GHz ISM band, providing for 5.5 Mbit/s and 11 Mbit/s. Parts of 802.11b provide backward compatibility and a fallback mode to allow interoperability with 802.11.

The available services allow DCF (Distributed Coordina-

0-7803-7442-8/02/$17.00 © 2002 IEEE

tion Function) and PCF (Point Coordination Function). Ad-hoc networks employ DCF, while access points within an infrastructure can use either DCF or PCF.

802.11b has a contention-free period (in PCF mode) and a contention period. The basic concept of PCF is polling. Polled stations can access the transmission medium without contention. This requires a base station, also known as an access point, to coordinate bandwidth assignment to the mobile stations.

The market for 802.11 and 802.11b interfaces and access points moves towards home consumer affordability, encouraging their use in the Future Home project. With a typical transmission power of 100 mW, the radio layers cover a typical home including garden. The infrared layer, on the other hand, is restricted to indoor applications and confined by the walls of the room, which can provide an advantage when it comes to eavesdropping.

Bluetooth

Bluetooth (Bt) is a specification [4][5] of the Bluetooth SIG for short-range RF communication. The goal of Bt is to replace cables between machines with wireless connection in space of approximately one room. Normal coverage of a 1mW Bluetooth transmitter is 10 meters, but with a 100mW transmitter, coverage of 100 meters can be obtained. The Bt chips are low-cost chips that also have low power consumption compared to technologies like 802.11 and HiperLan/2. Low power consumption makes Bt especially suitable for portable devices. Bt supports point-to-point and point-to-multipoint data and voice communication. Bt operates on the 2.4 GHz unlicensed frequency band.

The communicating devices form a so-called piconet. One of the devices becomes the master of the piconet, while the others are slaves. There can be maximum 7 slaves simultaneously receiving from or transmitting to the master. In addition there can be 248 slaves that are in the park or hold mode. Park and hold are low-power, connected modes from which a slave can start participating within 2 ms.

The maximum data rates for an asymmetric data channel are 57,6 and 721 kbps. For a symmetric data channel the maximum data rate is 432,6 kbps to both directions. For voice streams, the data rate is 64 kbps. Maximum three simultaneous voice channels or one channel with asynchronous data and synchronous voice are possible, simultaneously. A steady stream of packets is ensured by the master that reserves time slots for the voice channels.

The receivers must know the pattern according to which the frequency is hopping. Thus the clocks of the communicating devices are synchronized to the master's clock and the frequency hopping pattern is defined by the master. The devices can freely join and leave a piconet. One device can belong to several piconets simultaneously. Such combination of piconets is called a scatternet. Each piconet has its own master and hopping pattern. The piconets are controlled by software, which can reside in any of the networked devices. In the Future Home approach, the HNSP would be the master and controller of the piconet.

The Bt specification also includes scenarios of the possibilities the new technology enables. These scenarios are called profiles, reflecting typical usage situations. They list mandatory and optional features that each device should implement in order to fulfill the interoperability requirements.

HiperLAN2

HiperLAN2 specifications have been developed by ETSI Project Broadband Radio Access Networks (EP BRAN) [13]. As a flexible Radio Local Area Network (RLAN) standard, HiperLAN2 is designed to provide high speed access (up to 54 Mbit/s) to a variety of networks including Ethernet, Internet Protocol (IP) based networks, Third Generation mobile core networks, Firewire IEEE1394 and Asynchronous Transfer Mode (ATM) networks. It can also be used for private wireless LAN systems.

HIPERLAN2 relies on cellular networking topology combined with an ad-hoc networking capability. It supports two basic modes of operation: centralized mode and direct mode. The centralized mode is used in the cellular networking topology where each radio cell is controlled by an access point covering a certain geographical area. In this mode, a mobile terminal communicates with other mobile terminals or with the core network via an access point. This mode of operation is mainly used in business applications, both indoors and outdoors, where an area much larger than a radio cell has to be covered. The direct mode is used in the ad-hoc networking topology, mainly in typical private home environments, where a radio cell covers the whole serving area. In this mode, mobile terminals in a single-cell home "network" can directly exchange data.

Basic applications include data, voice and video, and specific Quality of Service parameters are taken into account. HiperLAN2 systems can be deployed in offices, classrooms, homes, factories, hot spot areas such as exhibition halls, and more generally where radio transmission is an efficient alternative or a complement to wired technology.

Performances of HiperLAN2 are unbeaten with respect to other equivalent standards. This is firstly a result of some specific mechanisms in the MAC layers. This gets then even stronger when HL2 is running in the direct mode, which makes it possible to establish a communication between 2 stations and interaction with the access point is not required.

ARCHITECTURE BASED ON IPV6

The terms that define the main characteristics of the architecture are wireless, heterogeneous and open. Furthermore, the objective is to connect the home to a global IPv6 network and access all the internal and external services through IP-based terminals.

The residential network will benefit from the new features of IPv6: address space, autoconfiguration, mobility support

and security. The whole system is tied together with a concept defined as Home Network Service Point (HNSP), which contains also functionality of a gateway and firewall. Thus, the home appliances and user terminals can communicate through secure IP-based intranet.

IPv6 Features

The Future Home platform is designed to use IPv6 [2] for connecting the terminals to services. Each computer connected to the Internet today has a fixed or dynamically allocated IP address. The address space of the current IPv4 is 32 bits (2^{32}). There is a shortage of address space already, because of the increasing number of computers connected to the Internet. With the introduction of the packet based, third generation cellular networks, also the mobile phones will be able to connect to the Internet and have an IP address.

The services built on the residential network must be always accessible, also remotely. Therefore, each home appliance and sensor will eventually have an IP address. Thus, the number of devices connected to the Internet will grow very rapidly and a bigger address space is needed. With introduction of IPv6, the address space increases from 32 bits to 128 bits.

However, this is not the only improvement IPv6 brings with it. It will also improve security of Internet, as data encryption and user authentication are built-in features of IPv6.

From home networking point of view, the IPv6 autoconfiguration feature is especially interesting. This feature guarantees automatic configuration of the network settings between devices and the network. In a home environment there often is a real need for autoconfiguration, since the users may not be able or willing to configure the system. A typical scenario for the user would be to add a new appliance to the residential network.

IPv6 also has features that contribute to faster network traffic. Quality of service (QoS) allows labeling of packets according to their contents. As a consequence, e.g., packets containing real-time video can be handled in routers with higher-than-default priority. The multicasting feature of IPv6 allows many clients to share one stream, meaning smaller load for the network. In the current IPv4 each client receives a separate stream.

Mobility support of IPv6 [3] allows a node to stay connected to Internet while moving from one place to another. There is no need to change the static IP address, information about the current location is sent to the home agent, which redirects the first packets to current location. After this the communication occurs directly between units and no longer via home agent.

Home Network Service Point

The Future Home project has defined a concept called the Home Network Service Point (HNSP). It defines the main functionality that is needed to manage a wireless residential system. The definition does not suggest that there merely should exist one home server but rather presents the basic services that should be provided to the system users and other system components. The basic services are listed in table.

Table 1: Description of the basic services provided by HNSP.

HNSP basic services	*Service description*
Authentication and authorization	System users, mobile terminals and external connections need to be properly authenticated and authorized before accessing the services
Logging	All software components of the system are able to generate events to be logged.
Registry	The home appliances and services are registered to enable service discovery.
Rule service	Simple automation tasks can be controlled using a rule based service component.
Loader	New and updated software components can be loaded and installed to the system.
Database access	Provides access for the users and services to the home system database.
System management	Home system Administrator may monitor and configure the system. Some of these tasks may also be automated.
Controlling and monitoring appliances	The home appliances can be contacted both locally and remotely.

The service architecture defines the logical components that are needed when users are interacting with the system and its services. The implementation details are out of the scope of the existing specification, but it can be foreseen that a middleware solution on top of the IP layer is needed. Figure 1 presents one viewpoint of the service architecture. The objective of the Future Home project is to find the most attracting features of the existing technologies (e.g. OSGi, UPnP and HAVi), and combine them to a working solution.

Appliances

The different home networking areas identified by the project include PC networks, home automation network with the household appliances, and the entertainment network with the audio/video equipment. With the heterogeneous technologies related to network and service levels, a solution based on adapters is presented.

For the household appliances e.g. the OSGi system bundles can act as adapters for powerline connected appliances. Similarly the PCs and printers can be connected and accessed through an UPnP system. Regarding the audio/video

appliances, it is essential to meet the real time constraints that exist in the transportation and distribution of the audio/video material (e.g. MPEG2 or MPEG4 streams). Because only IEEE1394 and HAVi are today capable to fulfill these real time transportation requirements, it is proposed to make use of a Home Media Server capable:

- On one hand to stream in and out audio/video material with respect to the real time constraints;
- On the other hand to interface with a bridging component. Such a bridge offers the usage of other transportation media like the IP protocols.

The common feature for all the appliance services is that they need to be accessible within the IPv6 based system. This is handled through the appliance adapters.

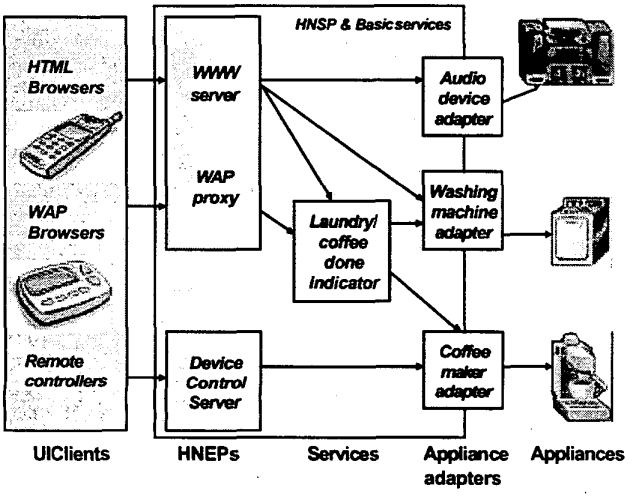

Figure 1: Depiction of the system service architecture with some example services and devices. The concept of HNSP defines how users can access the services and appliances through Home Network Entry Points (HNEP). In addition all the basic services defined will interact within the HNSP.

Terminals

At the home there will exist both fixed and mobile terminals. The terminals are used to access the internal and external services provided by the system and service providers. Furthermore, all the appliance user interfaces can be seen as services. The terminals are mainly operated through graphical browser interfaces.

Essentially, fixed AV terminals are large displays offering high quality of rendering. The issue to be solved for such terminals relates to the capabilities of running simultaneously several different functions:

- Real time MPEG2 AV decoding,
- Rendering of user interface pages, which give access to external services or control in home appliances.

The solution pursued here is to combine Firewire/HAVi features with IP based tools; therefore, terminals in the Firewire cluster and running the HAVi interoperability layers include some specific extensions for running HTML browsers in relation with HTTP servers.

On the other hand terminals with Ethernet access and IP stack are intrinsically capable of HTML and HTTP operations but will be equipped with decoding means to have full audio/video terminal capabilities.

Mobile terminals include PDAs, remote controllers and mobile phones. The mobility of the terminals can be managed through IPv6 mobility support. In addition, the terminals are authenticated by the HNSP whenever a new connection is required. For some type of terminals this is required only ones (e.g. for remote controllers).

SECURITY, PRIVACY and MOBILITY ISSUES

Residential networks can be very vulnerable and exposed to attacks, especially when they are connected to public networks like the Internet. Security issues are often very similar to intranets of companies and other organizations. Furthermore, privacy is something that concerns everybody when home and personal life are under consideration.

The following sections discuss the different available security issues and solutions for wireless residential networks, and present also subjects related to mobility of home users.

Network level encryption and Overhearing

802.11 WLAN provides WEP, the Wired Equivalence Privacy, with basic authentication, access control, and confidentiality services. However, a number of vulnerabilities have become known recently, allowing to compromise all these three security claims of WEP [11], [12]. For the Future Home project this implies to use additional security layers, at least for sensitive data (e.g. data that could physically open doors or bank accounts, in contrast to entertainment).

In Bluetooth, the frequency hopping keeps different piconets separate. However, in some cases it is necessary to hide the data that is being sent. The Bt generic access profile [5] (minimum set of services) defines three security modes are 1) non-secure, 2) service level security and 3) link level security. In mode 3 Bt initiates the security procedures in lower layers, before the channel is established. Other Bt devices can be marked as 'trusted' or 'untrusted' in the Bt security manager's device database [6]. In addition to this, access rights to each service can be defined as one of the three possibilities: 1) open to all, 2) authentication needed, 3) authentication and authorization (checking of access rights) needed. A trusted device has access to all services. The Bt security features have been criticized [7], so improvements are necessary before sensitive data should be transmitted over Bt.

HiperLAN2 provides two security services: confidentiality and authentication. These services and the used algorithms are negotiated during the association session. First, to ensure confidentiality, HiperLAN2 may use DES or 3-DES. The encryption key is obtained dynamically using the Dif-

fie-Hellman key exchange protocol. Second, two authentication mechanisms are available: 1) Hash-based authentication using a previously shared key between pairs 2) RSA authentication using Public Key Infrastructure and digital signature. Authentication may be unidirectional or bi-directional. Authentication takes place after encryption, if any. Consequently, it may be protected from eavesdropping when required.

Network Interference

An upcoming issue in the radio physical layer is the interference between wireless technology. 802.11 and Bluetooth share the same 2.4 GHz band, and apply similar Frequency-Hopping schemes. However, the hopping frequency of Bt is much more rapid, and the packets are much smaller in size. In consequence, a single small Bt packet collides with a long 802.11 frame, and quickly changes the frequency, so that the Bt transmission experiences only little interference, while the 802.11 suffers severely.

In HiperLAN2, the Dynamic Frequency Selection allows negotiation of frequencies so that co-located networks will use different frequencies and can avoid interference between them.

IPSEC and IPv6 Mobility support

Encryption on the network layer is required always when a wireless terminal or appliance is communicating. This can be handled using IPSEC, which is an integral part of IPv6. The keys can be based either on public key cryptography or on shared secrets. The aim is to have a virtual private network between a service and a device.

Through key management, the devices can also be authenticated even when they are mobile. When this paper was written the IPSEC specification was a work progress. Especially, the key management is not fully defined and that would suggest using shared secrets, since they can be managed internally, e.g. by the HNSP.

Using IPv6 mobility support, the mobile terminals can be registered at their home location, and at the same time be assigned the necessary keys.

User and terminal authentication

Users and terminals need to be authenticated and authorized every time the system is accessed. From the user point of view this must be as transparent as possible. Strong authentication is needed to ensure privacy of users. Authentication and authorization components can be built in a way that they intelligently and flexibly allow secure usage of the services.

Strong authentication mechanisms can be based on electric identities, shared secrets, biometric identification, etc. In addition user profiles are used for creating user groups to access certain classes of services. Mobile terminals are often analogous to banking cards: they are personal and can be accessed using a pin code. When these terminals are registered to the home environment, shared secrets can be uploaded there, which can then be used for terminal (and user) authentication and data encryption.

CONCLUSIONS

Residential networks that fulfill the requirements of home users are yet to come. Seeing the home environment as a part of Internet suggests an intranet based solution, familiar to all existing business organizations. Existing technologies can be integrated using IPv6 to provide a manageable wireless local area network.

REFERENCES

[1] Future Home System Architecture Specification, Deliverable D22: Wireless Home Network Architecture and Concepts for User Interactions, http://future-home.vtt.mediapoli.com/fh/public

[2] Deering, S., Hinden, R., Internet Protocol, version 6 (IPv6) Specification, RFC 2460, Dec 1998.

[3] Johnson, D.B., Perkins, C., Arkko, J., Mobility Support in IPv6, Internet Draft (work in progress), draft-ietf-mobileip-ipv6-17.txt, May 2002.

[4] Bluetooth SIG, Specification of the Bluetooth System – Wireless connections made easy – Core, version 1.1, http://www.bluetooth.org/, 22 Feb 2001.

[5] Bluetooth SIG, Specification of the Bluetooth System – Wireless connections made easy – Profiles, version 1.1, http://www.bluetooth.org/, 22 Feb 2001.

[6] Bluetooth SIG (Müller T. et al), Bluetooth Security Architecture, version 1.0, 15 Jul 1999.

[7] Vainio J.T., Bluetooth Security, Helsinki University of Technology, http://www.niksula.cs.hut.fi/~jiitv/bluesec.html, 25.5.2000

[8] ANSI/IEEE Std 802.11: Local and metropolitan area networks - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE, 1999 Edition

[9] IEEE Std 802.11a-1999: Local and metropolitan area networks - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - High-speed Physical Layer in the 5 GHz Band, IEEE, 1999 Edition

[10] IEEE Std 802.11b-1999: Local and metropolitan area networks - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Higher-Speed Physical Layer Extension in the 2.4 GHz Band

[11] Weatherspoon, Sultan: Overview of IEEE 802.11b Security. - Intel Corporation, http://www.intel.com/technology/itj/q22000/pdf/ art_5.pdf, August 2001

[12] WEP Security Statement. Wireless Ethernet Compatibility Alliance, http://www.wirelessethernet.org/pdf/20011015_WEP_Security.pdf, September 2001

[13] ETSI BRAN Specifications for HiperLAN2, http://portal.etsi.org/bran/kta/Hiperlan/hiperlan2.asp

[14] HiperLAN2 Global Forum, http://www.hiperlan2.com