Challenges in Efficient Realtime Mobile Sharing

Dennis J.A. Bijwaard, Henk Eertink, and Paul J.M. Havinga

Abstract. Future applications are envisioned to be adaptive to various changes in network, environment and situation. These so-called pervasive applications will be composed from both locally and globally available multimedia resources such as audio and video, web services and context sources. The rapidly increasing pervasiveness in todays networks, i.e. the number of mobile devices, the amount of data they generate and share (near) realtime increases rapidly. In fact this forms the basis for research efforts on the Internet of Things. The increased pervasiveness leads to numerous efficiency and scalability challenges. This chapter will detail the state of the art and binding concepts for efficient realtime sharing and mobility of multimedia and context. Additionally, it lists the associated challenges and their progress in a number of research projects.

In the past decade we have seen a number of technology boosts. Multimedia like audio and video moved from analogue to digital, enabling free audio/video calls over the Internet. Multiple network types have been integrated into mobile devices and bandwidth is gradually increasing. Sensors became wireless and form wireless sensor networks for environmental monitoring, and multiple sensors are added to mobile devices enabling different interaction modalities and situation awareness, The number of mobile devices and their capabilities are gradually increasing, and server clouds have been created that offer remote processing and storage.

Dennis J.A. Bijwaard
Inertia Technology, Enschede, The Netherlands
e-mail: `dennis@inertia-technology.com`

Henk Eertink
Novay, Enschede, The Netherlands
e-mail: `Henk.Eertink@novay.nl`

Paul J.M. Havinga
The University of Twente, Enschede, The Netherlands
e-mail: `P.J.M.Havinga@utwente.nl`

N. Bessis et al. (Eds.): *Internet of Things & Inter-cooperative Comput. Technol.*, SCI 460, pp. 115–142.
DOI: 10.1007/978-3-642-34952-2_5

As a result, today's connected networks enable feature-rich applications that adapt according to situational and environmental changes, and the networks and objects that are encountered. Some currently available applications already adapt according to changes in the environment and the situation that the user is in, examples are: route-planners that adapt to traffic conditions along your route, games that react to movement of a handled mobile device, mobile devices that automatically connect to wireless networks that are in reach.

However most of current adaptive applications are dedicated to a single task, and there is only limited sharing of information between applications of different vendors. Furthermore, the performance of applications is often determined by the polling frequency of mobile devices and by the server-side capacity, which is often consumed by distributing the same information to many mobile devices. At the same time, the mobile devices change network and can be temporarily without network. Efficient sharing of multimedia content is nowadays limited to that of dedicated content providers, and the content is not seamlessly continued when changing access network.

Future applications are envisioned to be adaptive to various changes in network, environment and situation. These so-called pervasive applications will be composed from both locally and globally available multimedia resources such as audio and video, web/cloud services and context sources. In fact all devices used in these pervasive applications are elements of the Internet of Things (IoT), all services are part of the Internet of Services (IoS), and all multimedia resources and services are part of the Internet of Media (IoM). Context sources in these pervasive applications can vary from your mobile phone's sensors to dedicated sensor networks deployed in buildings and vehicles, sensor nodes attached to beings and objects, and events generated from devices and applications. Higher level context can be obtained by reasoning based on this sensor information and events. Important prerequisites for interoperability of different services are identity federation for usage of cooperating services, standardisation of discovery and usage interfaces. A prerequisite for context gathering in the IoT is the geographical location where context is gathered. This location often has to be deduced from the environment of a moving entity (e.g. a complete sensor network can move while only one node has Global Positioning System (GPS) support).

Example pervasive applications are sharing your live video with large group of mobile users, automatically switching received video on your mobile to a bigger screen nearby and adjusting nearby light levels for advanced viewing, realtime access to shared context information independent of your current network connection.

Current enabling technologies like Web 2.0, Grids, P2P, and cloud computing may not be sufficient to enable the multitude of mobile users and applications to use and share realtime multimedia content, and context information like sensor network information over the Internet. Also composing pervasive applications from multimedia, web/cloud services and context sources still holds many challenges.

The underlying problem is the rapidly increasing pervasiveness in todays networks, i.e. the number of mobile devices, the amount of data they generate and share (near) realtime increases rapidly. This leads to numerous efficiency and scalability challenges.

This chapter will detail the state of the art and binding concepts with respect to efficient realtime sharing and mobility of multimedia and context, the associated challenges and their progress in a number of research projects. First, mobility and sharing in heterogeneous networks (including sensor networks) (see Section 1) and multimedia (see Section 2 will be described. Next service platforms handling mobility and roaming (see Section 3), and pervasive service platforms (see Section 4) that enable composed services from web, context and multimedia services. This chapter concludes (see Section 5) with the challenges and research progress for efficient realtime mobile sharing.

1 Heterogeneous Networks

In this section we describe different networks that enable users access to the Internet via their devices (See Section 1.1), and Wireless Sensor and Actuator Networkss (WSANs) (see Section 1.2) that gather information from the environment and allow actuation in that environment. User devices and WSAN nodes play an important role in the IoT.

1.1 IP Networks

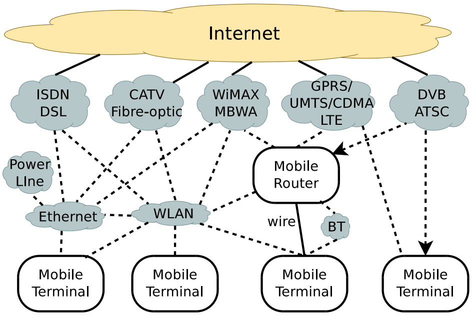
In the beyond-3G environment of today, users have access to an increasing number of different access networks, both wireless and fixed. The combination of fixed and wireless networks enables end-users to be almost always on-line and connected to their preferred network(s).

Beyond 3G-environments include beyond 3G-networks (also called Next Generation Networks (NGN)) as well as next generation terminals and services. Beyond 3G-networks consist of a variety of wireless and wired networks as core and access networks. End-user terminals and service providers are the end-points of these networks. Global IP-connectivity exists between all these networks and all end-to-end communication is IP- based. See Figure 1 for a number of IP connectivity options including unidirectional broadcast networks. Note that multiple access networks can be used simultaneously (multi-homing). With a mobile router, a mobile data connection can be shared with other devices over wireless technologies like Wireless LAN (WLAN) and Bluetooth or wired. When doing this with a mobile terminal this is often called tethering. This creates a potentially moving network, e.g. when used in a train.

In the next subsections we describe transparent mobility with Mobile IP, IP data flows, and broadcast/multicast/unicast.

1.1.1 Mobile Internet Protocol

Mobile IP [35, 28] (MIP) allows transparency of network changes and allows to maintain all TCP/IP connections while changing networks. MIP is mostly beneficial



ATSC	Advanced Television Systems Committee
BT	Bluetooth
CATV	Cable TeleVision
CDMA	Code Devision Multiple Access
DSL	Digital Subscriber Line
DVB	Digital Video Broadcast
GPRS	General Packet Radio Service
ISDN	Integrated Services Digital Network
LTE	Long Term Evolution
MBWA	Mobile Broadband Wireless Access
UMTS	Universal Mobile Telecommunications System
WLAN	Wireless Local Area Network
WiMAX	Worldwide Interoperablity for Microwave Access

Fig. 1 Different IP connectivity options

for connections with longer duration. A lot of tasks on mobile devices (such as web browsing and fetching/sending email) are not troubled so much by network changes since they are done rather quickly and can be easily be repeated when they happen to tail by a network change. Mainly longer sessions like Virtual Private Networks (VPNs), large up/downloads, and multimedia sessions need to be maintained while changing networks.

Mobile IPv4 [36] is the IETF standard for supporting mobility at the network layer in IPv4 networks. The terminal denoted as the Mobile Node (MN) gets a home IP-address assigned to be used for all communications. When the MN is not in its home domain, a so-called Home Agent (HA) forwards (tunnels) traffic to the MN's current location in a foreign network. In the foreign network, the MN obtains a Care-off-Address (CoA) from a Foreign Agent (FA) or a DHCP server, resulting in a FA-CoA (which is the address of the FA itself) or a co-located CoA, respectively. A co-located CoA has the advantage that an FA is not required in every visited network. Each time an MN changes its CoA it must re-register it with its HA in order to receive traffic directed to its home IP-address.

Mobile IPv6 [28][37] addresses a number of the Mobile IPv4 shortcomings such as the triangle routing problem. Route optimisation in Mobile IPv6 circumvents the triangle routing problem by sending binding updates, containing the current CoA of the MN, from the HA to all correspondent nodes.

Extensions have been proposed to Mobile IP to also handle moving networks with Network Mobility (NEMO). Examples of such moving networks are trains and planes that share their connection to a celular network like Universal Mobile Telecommunications System (UMTS) with the people they transport.

1.1.2 IP Data Flows

Communication in heterogeneous networks is a combination of data flows between applications. These data flows can be connection oriented with protocols like Transmission Control Protocol (TCP) and Stream Control Transmission Protocol [46] (SCTP) or connection-less with protocols like User Datagram Protocol (UDP).

These flows can be protected from eavesdropping using security measures, and their quality can be maintained using Quality of Service (QoS) measures.

Security of IP data flows can be done at multiple layers of the TCP/IP model:

- at the network access layer by encrypting the packet payload
- at the Internet layer by using Internet Protocol Security [29] (IPsec)
- at the application layer by using protocols like Secure Socket Layer (SSL) and Transport Layer Security [21] (TLS) for secured bidirectional connections, and Pretty Good Privacy [17] (PGP) for securing individual messages.

In order to provide QoS, packets of separate IP flows can be classified differently (e.g. as best-effort, audio and video), such that they can be treated properly in the network. QoS treatment involves all network layers in every network element in the communication path, as illustrated in Figure 2. End-to-end QoS is determined by the lowest weakest link among all network elements between sender and receiver, and end-to-end QoS can be solved by dividing the problem along network domain boundaries [32], as illustrated in Figure 2.

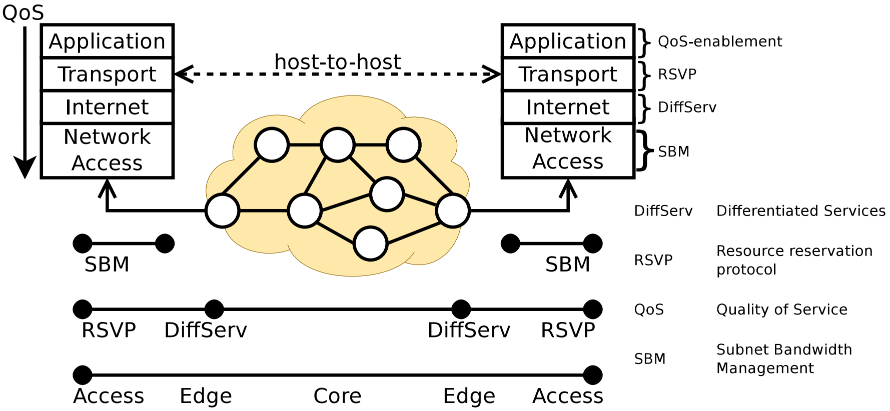


Fig. 2 End-to-end QoS across access, edge and core domains

1.1.3 Digital Broadcast, Multicast, Unicast

The main difference between broadcast, multicast and unicast is that broadcast is destined to everyone that is able to listen. Multicast is for a selection of listeners, and unicast is directed to a specific listener. A distinction can be made between bidirectional broadcast in which the same (wireless) medium can be used to send something back and unidirectional broadcast that is only one way. Unidirectional broadcast can use a return channel on another access medium to send something back.

Traditional broadcast uses (radio) technologies to broadcast content to a large number of users, such as analog audio channels and Television (TV) via the air or via cable, and the last decade digital broadcast gradually became the new standard with mainly Digital Video Broadcast (DVB) and to a lesser extend Advanced Television Systems Committee (ATSC).

In fixed telephony, any of various Digital Subscriber Line technologies (xDSL) is used for multicasting television to the end-users and offering interactivity with Internet Protocol television (IPTV). Broadcasting all channels is not really an option in xDSL since the last hop to the user is the dedicated twisted pair phone line which currently only supports high data rates over small distances.

In the mobile telephony standards UMTS and Code Division Multiple Access (CDMA), Multimedia Broadcast Multicast Service (MBMS) offers multicast and broadcast on handsets and via data cards (e.g. for laptop). MBMS is an enhancement feature of the UMTS architecture aiming at providing the capability for Broadcast and Multicast Services in the network (under Release 6).

DVB is availabe in a number of types, including DVB-Satelite (DVB-S), DVB-Cable (DVB-C), DVB-Terrestrial (DVB-T), and Digital Video Broadcast - Handheld (DVB-H). All DVB data and digital data in ATSC is transmitted in Moving Picture Experts Group (MPEG) transport streams, which enables transmission and storage of audio, video, and data.

There are basically two types of multicast over IP, namely Source Specific Multicast [12] (SSM) and Any Source Multicast [19] (ASM). In ASM the user expresses its interest in a specific multicast group, in SSM, the user expresses interest in a combination of a specific source and multicast group. In both cases the routers between the source and destination need to make sure that the users that joined the multicast group get the associated IP streams efficiently (without unnecessary duplication).

1.2 Wireless Sensor and Actuator Networks

A WSAN typically consists of a large number of low-power sensor and actuator nodes. These nodes are equipped with a wireless transceiver, a small microcontroller, a power source and multi-type sensors such as temperature, humidity, light, heat, pressure, sound, motion, etc. Additionally, the nodes can be equipped with actuators such as Light Emitting Diodes (LEDs), switches, and even motors. WSAN nodes are some of the smaller devices in the IoT that collectively generate context information that can enhance pervasive applications. When these WSANs also have processing capabilities, they are also referred to as Pervasive Systems, i.e. systems containing a large number of collaborating tiny sensing, actuating, routing, and processing devices.

WSANs are commercially available in various forms, shapes, sizes, and functionality running various operating systems (e.g. TinyOS [16] or AmbientRT [26]). Interaction between sensor nodes and applications has not yet been standardized.

Applications involving WSANs are very diverse and involve one or a combination of various types of sensor networks. We can identify at least six types of wireless sensor networks, namely (based on [31]):

- **Environmental Sensor Network (ESN):** These are the very first type of wireless sensor networks. Traditionally, ESNs were solely deployed for monitoring and data collection purposes. ESNs are often large scale, static, non-dense, and are deployed in harsh and unattended environments. Energy efficiency, long network life-time and security have always been the major concerns of ESNs.
- **Body Sensor Network (BSN):** BSNs are sensor networks consisting of few wireless sensor nodes on or around a living being's body connected to a more powerful device such as a smart phone. Monitoring of vital signs, tracking, and data collection have been the main objectives of these sensor networks. Interaction with sensor-enabled objects [15], such as a dumbbell or ball, is an interesting upcoming usage area. BSNs are small scale, use different types of sensors and are usually limited to single-hop wireless communication. Since personal information can be collected by these networks, both security and privacy are major concerns.
- **Structure Sensor Network (SSN):** SSNs consist of medium to large numbers of wireless nodes usually attached to or in buildings (e.g., office), structures (e.g., bridges), infrastructure (e.g., rails) or deployed in specific venues (industrial sites). Wireless nodes can also be attached to objects moving inside the structure and between structures. SSNs usually extend their wireless coverage with multiple hops of wireless communication and often use a variety of sensors.
- **Transport Sensor Network (TSN):** Transportation means such as cars, trucks, and trains, have a number of sensors. Over the past few years, many efforts have been directed towards wireless communication and networking between transportation vehicles (e.g. vehicle to vehicle communication via IEEE 802.11p). Each individual vehicle can be seen as a sensor node, which locally observes its own state while it also monitors its surroundings.
- **Vehicle Sensor Network (VSN):** The sensor data from within a moving vehicle (e.g. a car, boat, train, plane) can also be transferred wirelessly (e.g. via General Packet Radio Service (GPRS)) to a central server, and be monitored remotely and/or merged with data from other sensor networks. In warehouse logistics, VSNs are often used together with SSNs, e.g. when monitored goods are transported in a truck from one warehouse to the other.
- **Participatory Sensor Network (PSN):** Mobile phones are becoming more and more equipped with sensors (e.g., GPS, accelerometer, gyroscope, camera) and different types of connectivity mediums (Bluetooth, wifi, Global System for Mobile Communication (GSM), etc.). This combination makes the mobile phone and in fact people carrying them a valuable source of collecting and transmitting information. Information collected by people through their mobile phones can range from personal health conditions and their trajectory to environmental conditions and pictures of the area in which they move around.

Mobility is typically covered within the WSAN, i.e. nodes within the WSAN can move around and use alternative nodes to stay connected. Mobility of nodes across WSANs and mobility of Internet-connected WSANs that are potentially used by multiple applications are still research topics.

The following application areas are considered [31], where WSANs are mobile and are potentially used by multiple applications:

- **Cool Chain Logistics:** In the cool chain market, it is important to optimise the quality of perishable products by ensuring optimal storage and transport conditions. In addition, assets can be tracked when they enter or leave certain areas.
- **Environmental/Habitat Monitoring:** Monitoring is done in the environment or the habitat of living beings, usually for extended periods where user-intervention is either expensive or disturbing. Data mules are sometimes used to collect the sensor information when no wireless coverage is available. In habitat monitoring also the animals themselves can wear a sensor node.
- **Surveillance:** Building, vehicle and infrastructure monitoring to detect forcefully opened or unlocked doors/windows, theft and damage.
- **Smart Spaces:** Smart spaces adapt to the needs of the users that enter and leave. They typically contain sensors and actuators that can be monitored and controlled by applications running in the environment and on user devices.
- **Remote eHealth:** In remote eHealth, sensor networks consist of few wireless sensor nodes on or around a living being's body. Typically, these nodes are integrated with a smart phone or a stationary device at home. Monitoring vital signs, and tracking are the main objectives of these sensor networks. Analysis is often done offline but increasingly becomes real-time.

Table 1 lists which WSAN types are typically used in each application area, and what items are mobile.

Table 1 Typical associations in specific application areas

Area /association	Cool chain logistics	Environment monitoring	Surveillance	Smart spaces	Remote eHealth
Mobile entity	truck, node	data mule, node	vehicles	user-device, object	user-device
Domains	depot, warehouse	geographic area	building, infrastructure	place	clinic
WSANs	areas, trucks	sub-areas	vehicles, areas, different types	different types	patients
Nodes	roll containers	sensor node	door, window	sensor nodes	sensors, objects
WSAN types	SSN, VSN	ESN	SSN, VSN	BSN, SSN, PSN	BSN
Apps	views, triggers	views, triggers	views, triggers	experiences	views, feedback

2 Multimedia Sessions

Multimedia sessions are sessions that contain one or more multimedia streams. In this Chapter we mainly focus on audio and video streams. Examples of multimedia sessions are Voice over IP (VoIP), audio/video teleconferencing, Video on Demand (VOD) and IPTV. Multimedia session enablers are part of the IoM.

This section first describes protocols for multimedia session control, then mobility for multimedia sessions and then compares multimedia session mobility with mobileIP.

2.1 Session Control

For controlling realtime multimedia sessions over the Internet between two or more parties, a number of standards are available, namely:

- The Real Time Streaming Protocol [44] (RTSP) supports video-like control over a multimedia session with a streaming server. It can for instance be used to establish, play, fast-forward, pause and stop a multimedia session containing multiple media flows;
- Revision 5 of HTML (HTML5) which is still under development supports playing audio and video files and is expected to support realtime multimedia playing in a web browser using RTSP.
- The Jingle [24] protocol extension to Extensible Messaging and Presence Protocol [42] (XMPP) enables signalling via an XMPP server for multimedia session setup;
- H.323 that uses telephony-style signalling from the International Telecommunications Union Telecommunications Sector (ITU-T);
- Session Initiation Protocol [11, 39] (SIP) using HyperText Transport Protocol (HTTP)-style signalling from the Internet Engineering Task Force (IETF);

Apart from those, closed approaches are available such as Skype and the flash player.

RTSP and HTML5 are mainly used for controlling unidirectional multimedia either from or to a streaming server and are not further considered. Jingle, H.323 and SIP do support setting up a multimedia session with multiple multimedia streams in any direction. Jingle does not support session mobility yet. There is one extension for session transfer [50] that has the deferred state. Jingle is designed to interwork with SIP. Because of the current lack of session mobility, this protocol is not further considered.

H.323 [27] is a standard published by the ITU-T for audio, video and data communication across IP networks. The H.323 Recommendation can be applied to voice-only handsets and full multimedia video-conferencing endpoints, and others. H.323 is part of the H.32X series for enabling video-conferencing across a range of networks including Integrated Services Digital Network (ISDN), Public Switched Telephone Network (PSTN) and IP networks.

H.323 does only provide seamless mobility while roaming when the network point of attachment does not change during handover (see recommendation H.510 from the ITU-T, e.g. when a mobility mechanism like MIP is in effect, or when all communication is tunnelled to the home provider network). H.323 is not further considered in the remainder of this Chapter.

SIP, as described in [43] and [41], is a signalling protocol used for establishing, maintaining, and terminating multimedia sessions and providing presence information in an IP network. Traditionally, resource discovery in SIP is done in a centralized manner, i.e. each domain has a local resource directory where all identities and their preferences are stored. SIP is adopted by the IP Multimedia Subsystem (IMS) of the 3rd Generation Partnership Project (3GPP) [1]. Peer to Peer (P2P) SIP, offers a distributed mechanism for resource discovery which can reduce (or even eliminate) the need for centralized servers. In the remainder of this chapter only traditional SIP is considered unless specifically stated otherwise.

SIP can, in addition, provide user mobility functionality because the identification of users with SIP is independent of underlying IP addresses. Wedlund and Schulzrinne in [49] proposed to use mobility support in SIP to support real-time communication. Most current SIP user agents on mobile terminal do not support these methods.

2.2 Multimedia Session Mobility

SIP has its own mechanisms for mobility management [49] for SIP-based applications as well as functionality for session adaptation.

Application layer mobility solutions, for example based on SIP, can either replace or complement network-layer mobility [45].

No single approach to IP mobility applies across heterogeneous applications in beyond 3G environments [33]. To meet the requirements of applications and deal with harsh networking environments multi-layered mobility management solutions and architecture are proposed, see for example [22] and [38].

2.3 Multimedia Session Mobility versus MobileIP

There have been a number of studies comparing SIP-based and MIP-based mobility management. The comparisons of the performance of the two protocols in [49] and [9] demonstrate that, in general, application-layer mobility management protocols, such as SIP, perform worse than lower-layer protocols in terms of hand-off delay, signalling overhead, and transparency. However, when suitability for deployment in next-generation networks is considered, it appears that SIP is a better mobility management solution for multimedia sessions, because it obviates the need for protocol stack and infrastructure changes [9]. A number of studies indicate that the suitability of a mobility management solution depends primarily on the type of application for which it is being considered. For long-lived TCP connections (such as FTP) and most standard Internet applications (such as Web browsing and chat), MIP offers a generic solution for roaming that seems to work well. However, for real-time applications, SIP is recommended [48, 49], because real-time applications (e.g., multimedia applications) have strict timing requirements that are not taken into account by MIP because it is a network-layer protocol. To optimize roaming behaviour, applications should be able to influence or even control the mobility management process, as they can when SIP is used as the mobility management solution. An additional benefit of using SIP for application-layer mobility management is that it allows applications to adapt their service behavior, based on the mobility management strategy selected, to provide the best possible end user experience.

3 Federated Service Platforms

Service platforms (see Figure 3) enable access to service providers to devices that are connected via heterogeneous networks. Federation between service platforms realises a service control layer. This layer enables third-party service providers to offer their services to roaming end-users, while being shielded from network-specific details. In addition, end-users with a Service Platform subscription can use the services to which they are subscribed while switching access networks (including foreign ones). The Service Platform adds value for functionality such as mobility management, session control, authentication, user profiles, and user localization.

We first describe the functionalities of service platforms, then further detail mobility management.

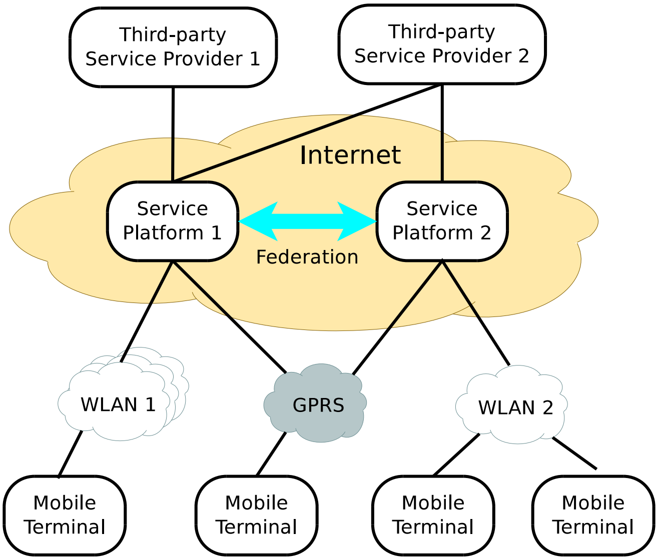


Fig. 3 Federated service platforms enabling services to mobile terminals

3.1 Functionalities

There are a number of different functionalities that a Service Platform can offer, among others:

- Bridging legacy systems: E.g. a multimedia gateway can be used to bridge telephony between GSM/PSTN/ISDN networks and VoIP.

- Providing identity across federated service platforms: a user has a home service platform and can use its identity to use foreign access networks and services provided by other service platforms. This federated identity is one of the prerequisites for the IoS.
- Multimedia and messaging: E.g. SIP application server, to handle voice, video, and messaging applications. This functionality is an enabler for the IoM.
- Charging: real-time and offline charging for services. Example charging types are time-based, volume-based, event-based.
- 3rd Party service interfaces: Example standards are the OSA/Parlay and their RESTful successors [8] for Telecom-based service platforms.
- Seamless use of different Access Networks: i.e. providing mobility management, see Section 3.2.

3.2 Mobility Management

To facilitate seamless continuation of services across access networks, users should be able to roam seamlessly from one access network to another and/or attach to multiple access networks simultaneously (multi-homing). Mobility management, which is the technical prerequisite for roaming behavior and service access, involves controlling the network(s) to which the user's terminal is connected and which service runs through which access network. I.e. mobility management discovers new access networks, and controls the handover between these networks [10]. It is also responsible for roaming services (e.g. continuous access to SMS and IP services). The services that can be supported on or across access networks depend on the characteristics (e.g., the bandwidth restrictions) of these networks; certain services may not be supported on certain networks. Therefore, it may be necessary to adapt ongoing service sessions to changes in the network environment. A typical example of such an adaptation is dropping video from an audio-video session for a low-bandwidth access network.

Mobility management plays a key role in dealing with user and terminal mobility in beyond 3G-environments. Following [6] and [7], mobility management can be defined as a functional component that firstly keeps track of the IP-addresses of mobile end-users, and secondly modifies the IP routes of the ongoing sessions of mobile end-users[1]. The mobile end-users' IP-addresses can be tracked per session. This Mobility management function enables other end-users to initiate new sessions towards the mobile end-user. Similarly, modification of the IP routes of ongoing sessions can be done collectively (for all sessions) or individually (per each session). Modification of active sessions is subject to the requirements of the sessions involved; examples of such requirements are minimal bandwidth and cost.

A mobility management system in the beyond 3G-environments described above has the following characteristics:

---

[1] A session can be an instantiation of a service that is established between two or more endpoints (i.e., users and/or machines). A more elaborate service concept is described in 4.1 and session concept is described in 4.2.

- Mobility management concerns[2] both user mobility and terminal mobility aspects. Therefore, the end-user (and not just her/his terminal) is the one whose mobility is tracked and handled by the mobility management.
- An end-user is likely to be associated with multiple IP-addresses corresponding to the active network interfaces of her/his terminal(s).
- Due to diverse requirements of heterogeneous applications in beyond 3G-environments, no single approach to IP mobility applies across these applications [33]. Therefore, the mobility management should provide multiple IP mobility solutions at different layers of the OSI model to handle mobility issues for services, individually or collectively.
- This asks for a multi-layered mobility management approach (i.e. mobility at different layers of OSI model) where the scope of the mobility management spreads from each individual service (and its sessions) to an aggregation of all services (and their sessions), associated with an end user. In other words:
    - The IP address to be tracked by the mobility management is the routable IP-address of the terminal interface, to which the end-user is attached for initiating a session of a particular service or any subset of services (this subset can include all her/his services).
    - The IP route to be modified by the mobility management corresponds to the terminal interface, via which the end-user is involved in an ongoing session or in any subset of ongoing sessions (this subset can include all her/his sessions).
- At any given time, the IP-address of an ongoing session of a service can differ from that for initiating a new session of the same service.

4 Pervasive Service Platforms

A pervasive service platform (see Daidalos [4]) offers user experience in addition to the Service Platform. This user experience can be composed from existing services and be personalized and situation aware, by utilizing sensor information, context, profiles, and history of the user and the environment. Even when the user is not connected itself, the pervasive service platform and services can act on behalf of the user. The context-aware and personalized service composition is an enabler for the IoS, and context-aware multimedia services are an enabler for the IoM.

Pervasive Service Platforms are a distributed form of pervasive systems that provide a home base for the users, and give them a digital identity at that base. Federation of platforms allows the user to communicate with users at other bases and use services provided at other bases. The federation of pervasive service platforms form an enabling middleware for the IoT.

Other forms of pervasive systems can be organized as peering components (see e.g. Hydra [23]) that can discovered and hooked-up dynamically, for instance when they get close to one another.

---

[2] A full solution involves the cooperation with other system functions like AAA, personalization, session control, etc.

In this section we describe the concepts for services, sessions, mobility and sharing in pervasive service platforms (see Daidalos deliverable DII-124 [5]).

4.1 Service Concept

A *service* is defined as a (potentially distributed) software application that provides certain functionality accessible via well-defined communication protocols. The type of service is defined by the offered functionality and the supported access protocols. Service sessions are running implementations of the service's functionality and protocols. According to this definition the type of a service is defined by the communication protocols it supports and the functionalities it uses and offers. This definition allows us to include a wide field of services including data services (e.g. a currency translator or email) and usage/configuration of hardware devices (e.g. a display or a printer). A service session is a concrete implementation of a service type that is actually running. Services often follow a traditional publish/discover/subscribe paradigm, meaning they are registered on a server, can be discovered by querying this server, and once discovered a service can be accessed directly.

Table 2 Pervasive Service requirements

Characteristic	Requirement	Short description
Discoverable	Required	A pervasive service has to expose its functionality, the supported protocols and its attributes in a standardised way, independent from the particular service discovery protocol. Nevertheless, it has to support at least one (e.g. SLP).
Composable	Required	A pervasive service needs to be able to cooperate with other services.
Context-aware	Optional	A service may be context aware, i.e. adapt according to for instance situational, network or environmental changes.
Personalisable	Optional	A pervasive service may be aware of the user's personal preferences, i.e. it may have parameters that can be personalised.
Private and Secure	Optional	A pervasive service may specify privacy and security requirements when accessing sensitive user-related data.

A *pervasive service* is a service that exposes its functionality and attributes in a standardized way, and is made available via specified service discovery protocols. The service can be integrated into a composite service. It may be security and privacy aware, context aware and allow for personalisation. Table 2 summarises the six requirements for a pervasive service.

The whole concept of the pervasive services is their adequacy as building blocks for more complex services, denoted as composite service: A set of cooperating pervasive services. A composite service may also be a pervasive service (recursive definition). A running composite service session is called a (composite service) session. Since service sessions that are being part of a composite service session, it may come and go frequently and necessary context information may change often, and therefore re-composition may need to be carried out regularly. During recomposition, service sessions might be added, reconfigured, removed or replaced by alternative ones. At a certain point in time the composite service session will be terminated, i.e. the composite service is stopped. During this process the individual services are disconnected and released. A composite service may also be called an application since the composite service provides the functionality to the end user. In order to create a composite service, knowledge is needed about how a composite service shall be created. This can be done both by the network provider, or by third parties.

4.2 Session Concept

When discussing data connections and streams it is necessary to describe the relation between the data packets, terminals, network nodes and services. This relation is usually known as a session, and may not always be easily identified (e.g. the set of packets under scope of a SIP application may not be identifiable by the traditional double set of IP addresses and ports). Another characteristic of a session is that it defines the relationship between a set of network nodes. For instance, a SIP session will involve a number of network nodes (SIP clients, SIP proxy) that are involved in the exchange of packets. The scope of what a session is varies with the aspect we are tackling. The following types of sessions are identified:

- **Network Access Session:** Between a device (mobile terminal) and a wired or wireless network. Especially for wireless networks, this usually involves authentication to the network.
- **Network Identity Session:** Includes all Network Access Sessions that use the same identity (or credentials) for authentication. This means e.g. having multiple virtual or physical interfaces on a mobile terminal authenticated using the same credentials.
- **Transport Session:** A transport session connects and/or exchanges data to and/or from a node in the network. Multiple transport sessions can exist within the same network access session, typical examples of transport sessions are TCP connections and UDP streams.
- **Application Session:** Contains (zero or more) transport sessions. Can exchange application-specific packets among distributed application parts. An important subtype of the application session is the multimedia session.
- **Pervasive Session:** A session that is directly mapped onto user goals and intentions. Can be context-aware and personalizable. Will control overall coordination of multiple application sessions that might interact with each other based on user context.

The following paragraphs further detail these session types.

Network Access Session

The network access session starts with authentication of the user identity and checking authorisation for its access from a given mobile terminal on a given network interface to a specific access network. When authentication is not necessary, the network access session starts by connecting to the network. The network access session ends when the network access is terminated on that network interface, which could be the case when a re-authentication is necessary in another network (e.g. for inter-domain mobility) or when the user logs off the mobile terminal etc. All other sessions have to be supported on top of these network access session(s).

In relation to the access technology, a network access session is always bidirectional, even when bidirectional technologies are being emulated using Unidirectional Link Routing (UDLR). Nevertheless, we can be have mostly unidirectional (e.g. authenticated + authorised broadcast access) or mostly bidirectional (e.g. wifi, UMTS, broadcast access + return channel, etc.) access. This does not preclude for a user with a DVB-enabled mobile terminal to access free information on the DVB broadcast, or, after registration, to keep on receiving protected content for a given time without any uplink (until registration times-out).

A network access session can have QoS guarantees as a whole, or for its contained transport sessions. Also both the whole session and the sub-sessions can have associated costs. The QoS guarantees and costs can differ when the network access session is handed over to another network, or to another mobile terminal. During a network access session, the Home Address (retrieved based on selected identity) of the interface will stay the same, and only the CoA will change after a handover.

Transport Session

Within a network access session, several transport sessions can exist, the most important ones are TCP, UDP and SCTP. TCP is connection oriented, is bidirectional and provides ordered reliable transport. TCP sessions have a clear start and end. UDP provides messaging over IP, and these messages can be combined into streams between the same sender and receiver(s). The end of a UDP session is much harder to determine and an UDP session is usually unidirectional (or multi-directional in case of multicast traffic). SCTP is message-oriented and can also ensure ordered and reliable transport like TCP, on top of that it supports multiple data streams in parallel within the same SCTP session and can support transparent failover in multihoming scenarios. SCTP sessions have a clear start and end like TCP.

While authentication and authorisation are never done on the granularity of a transport session, QoS control and mobility management are typically referring to transport sessions. In case of a handover between different domains that requires re-authentication, a transport session will typically continue, while the related network access session changes.

Network Identity Session

A network identity session contains all concurrent (i.e. overlapping in time) Network Access Sessions that use the same identity for authenticating to the network(s). The same identity can be used for connecting to different physical interfaces using different technologies, or to different logical interfaces on the same physical interface. As long as the Network Access Sessions use the same identity they are considered to be part of the same network identity Session.

Application Session

Over these access sessions, applications are running their own sessions. One example of an application session is a multimedia session; other examples are broadcast services, context services, web services, and simple applications like telnet and ftp. The simple applications and web services are more traditional sessions, and easier to identify. The complexity of application sessions is reflected in complex services, even if not multimedia. Other non-multimedia sessions may cover services such as lookups for a restaurant, or cinema, access to traffic (jam) data, or download of audio/video content for offline consumption (e.g. buying songs on iTunes). Some of these services may actually relate multiple applications, and involve changes of many connections and/or connection end-points. For those application sets an application session is comprised of all data transactions which take place until a service transaction (e.g. buy and download an mp3) is finished.

Any kind of control traffic (like multimedia session setup, RTCP control messages, TCP acknowledgements) related to an application is part of the application session (typically consisting of several transport sessions), and that applications sessions may as a whole be subject to mobility and QoS management. The level at which this can be globally handled depends on the specific session characteristics. The multimedia session is further detailed below.

Multimedia Session

A multimedia session (see also Section 2) can be established between two or more endpoints (users or service). The session usually starts after an invitation of a participant is accepted by another participant. A multimedia session can contain a number of multimedia streams and connections between the endpoints (usually audio, video and/or instant messaging), and session-specific messages (signalling) can be exchanged between the session participants. During the session a number of things can change:

- Multimedia streams/connections can be dropped, added or moved to other endpoints (partial session mobility)
- Quality of multimedia streams/connections can be changed
- Endpoints of the session signalling can change network location
- Endpoints of the multimedia streams/connections can change network location (e.g. handover or load-balancing when multihomed)
- Endpoints may join or leave the session
- Session may be transferred to another endpoint.

A multimedia session usually contains a control session on the control plane that defines and controls media session endpoints on the data plane. Figure 4 shows how the control session on the control plane and the media session endpoints at the data plane are related to each other for a typical audio/video session between a mobile node and a correspondent node.

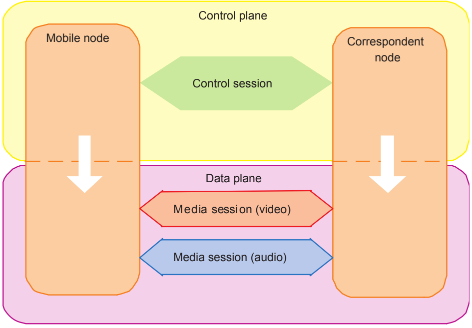


Fig. 4 Multimedia session with control, audio and video sessions

Pervasive Session

A pervasive session, in its simplest form, can be considered a collection of application sessions, both multimedia and web service (or other) sessions. A pervasive session will run a pervasive service, where the different parts of the service can be engaged in different application sessions (e.g. in a multimedia session and/or FTP session). Note that a Pervasive Session is contained inside an identity session. A pervasive session converges application sessions for a specific user experience, where the convergence is guided by the application logic needed to satisfy the user needs. So, while most connections and streams in a pervasive session could be setup by application sessions like the multimedia session, the pervasive session also contains the logic for context-aware starting and stopping of these sessions, adaptation of itself and its parts.

As an example consider a unified conferencing (UC) pervasive service (running in a network node) that is in charge of supporting virtual meetings between three persons in any possible way (depending on the communication technology that is available at any given context for the two people). If initially person A wants to use UC to meet person B there are different scenarios that can be supported by UC:

- Both A and B have mobile phones available to them and can be engaged in a phone conversation. In this case UC could set up a SIP session between A and B.
- While engaged in the SIP-based voice session, A and B might want to share a document. UC might initiate an FTP session or issue a SIP instant message to allow A send a file to B, and later to set up a data conferencing session where A and B can collaboratively browse through the document.
- If A or B’s context changes in such a way that one of them gets access to a video camera (e.g. after having moved to another room while in the conference) UC might decide to add a video session to allow A or B see the other party.
- A third person C comes into the conference. C has access to only a chat program. UC might choose to add a speech-to-text conversion session so that C can participate in the conference without disturbing the conversation flow.

- UC might detect that C cannot receive documents on FTP and does not have any document sharing tool available. UC might decide in this case to print the document under discussion to the printer that is located close to C.

The above example shows many characteristics of a pervasive session. UC comprises a pervasive session that implements a multiparty conference among three people. This conference session can be regarded as an overlay application session that is continuously initiating other application sessions depending on the needs of the conference. For all these sub-sessions, the pervasive conference session keeps track of states of the different nodes, is informed about new nodes (e.g. a printer) becoming available, etc. An extended definition of a pervasive session might include application-initiated management of network access and transport sessions. It is easy to see the usefulness of such a concept. For instance, UC above could be extended to make active use of interface selection in order to set up and tear down network access sessions. As long as none of the participants in a conference have access to multimedia tools, UC might choose to use a low-bandwidth low-QoS network connection. Once users get access to multimedia, UC might choose to initiate network access and transport sessions to use better quality network available.

To summarize, a pervasive session has the following properties:

- It is a session that is often long-lived. I.e. it might live in the background and respond to stimuli from its surroundings (e.g. start an application session when there is a context change).
- It is heterogeneous, and will contain different types of sub-sessions. In its simplest form, these sub-sessions will be all application sessions. In its extended form, sub-sessions might also include network access and transport sessions. The pervasive session is the overlay session that manages the sub-sessions.
- It might include resources from different administrative domains. This means that setting up and tearing down sub-sessions might involve federation, authentication, etc.
- It will have several states. It might be running (actively using resources), suspended (not reacting to any stimuli), waiting (in the background, reacting to stimuli) etc.

4.2.1 Session Relationship Example

Figure 5 gives an example of intertwined session relationships. It shows that a *network access* session can exist for different access technologies and that all *network access* sessions for one identity are within the same *network identity* session. It also shows that an *application* session can potentially contain multiple *transport* sessions, e.g. a multimedia session (e.g. S3) can contain both a multicasted UDP stream and a TCP connection for signalling via different access technologies (DVB-X + GPRS), a broadcast session (e.g. S1) can contain multiple multicasted UDP streams, and a WebService session (e.g. S5) can contain one or more TCP connections. A context service (e.g. S10) can get context from *application* sessions, sensors on a user device and sensor networks connected via different identities

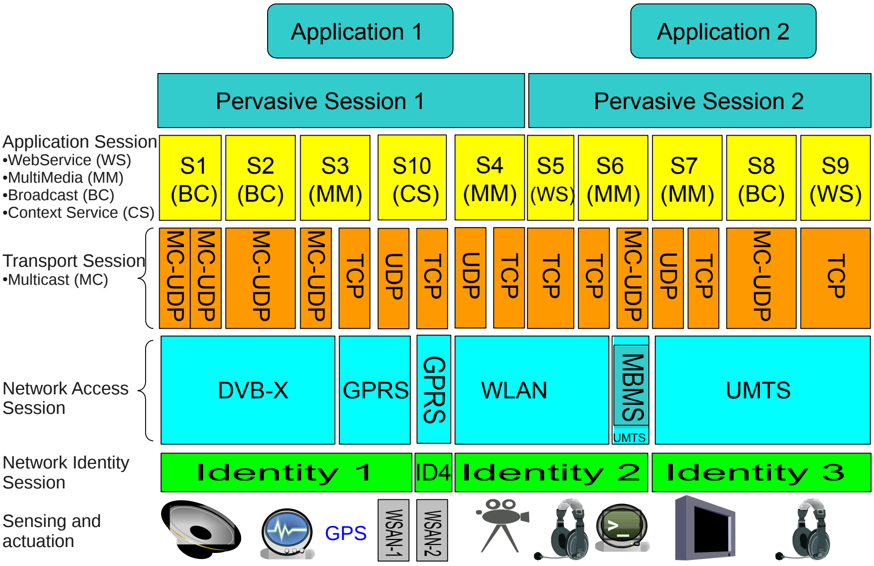


Fig. 5 Example Session relationships

(e.g. identity 1 and 2 over GPRS) and offer this context information or an inferenced version thereof for usage in all constituents of a pervasive session.

At a higher level, Application 1, could start Pervasive Session 1 which contains multiple Application sessions, namely S1, S2, S3, S4 and S10. Application 2 could start Pervasive Session 2, containing Application sessions S5, S6, S7, S8 and S9.

Regarding the relationships above, a set of information is needed in order to keep the overall complex view consistent at runtime. Some of the needed shared information is listed here:

- Identity-related information: The identity used to form a *network access* session will be used for associated *transport* sessions. Utilizing the service platform as an identity provider, this (network) identity could also be re-used by the *applications* and *pervasive* sessions within the *network access* session. However, the identity for those *application* sessions does not need to be shared.
- Preference outcomes: Preferences for using a Network Access Session might depend on the Application Session running on top of it. This information needs to be communicated.
- Context information: Context information might affect how lower-level sessions are configured. Moreover, access to different *network access* sessions might guarantee or deny access to different sets of context sources.

4.3 Mobility

A distinction is made between the following types of mobility:

- **user mobility**, a user can access the network from multiple devices, i.e. the user actually is able to connect and act in a seamless way from all mobile terminals.

- **device mobility**, a device can change its attachment point to the network, i.e. it handles mobility of network access sessions between different access networks. When re-authentication is necessary, the change from one network access session to another would also be considered terminal mobility (but may not be considered seamless and may break running sessions).
- **interface mobility**, a session can be moved from one interface to another in the same device.
- **service mobility**, the provider of a service can be moved during the provisioning of that service.
- **session mobility**, a session or its parts can be transferred between devices.
- **WSAN node mobility**, a node moves within the WSAN or between WSANs.
- **WSAN mobility**, the WSAN may move and therefore change its network point of attachment (device mobility) or change to another network interface (interface mobility).

Different abstraction layers can be considered, both on the network side and the terminal side to abstract technology specific issues, enabling both local and remote communication for enhanced handover procedures. Handover can be initiated either by the mobile node (mobile initiated handover) or by the network (network initiated handover). More advanced concepts such as network aided mobile initiated handover can also be considered.

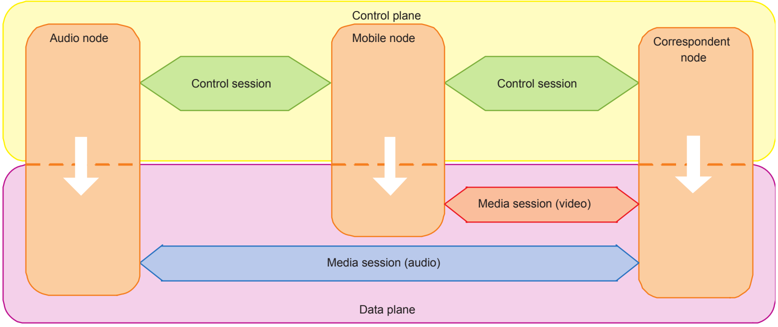


Fig. 6 Audio stream endpoint moved from Mobile Node to Audio Node

Session mobility can be related to mobility of: network access sessions, transport sessions, application sessions and pervasive sessions with associated transport sessions (streams and network connections). Since application and pervasive sessions can be composed of sub-sessions and services that use multiple network access sessions, session mobility can have many aspects, and may cover several of the above mentioned mobility types:

- **Network Access Session Mobility:** the network access session is changed from one network interface to another, or is moved to another device. This would require support for multihoming from the network access provider.

- Transport session mobility: a transport session is moved from one interface to the other or between devices.
- **Partial Session Mobility:** either signalling/control or contained connections/ streams move
  - Multihoming: part of a session moves from one to another network interface
  - Multi-device: part of a session moves from one device to another device (see Figure 6)
- **Full Session Mobility:** the whole session moves
  - Multihoming: The whole session, including signalling, is moved from one interface to another.
  - Multi-device: The whole session, including signalling, moves to another device.
- **Service Session Mobility**
  - Multihomed service session: Part of a composed service session moves from one to another network interface of a device (could be service session on 3rd-party server or on terminal).
  - Part of a composed service moves from one device to another device (could be 3rd-party service or service on terminal)
  - When moving to another domain a candidate service can be instantiated in that domain when the user, personalisation, or context indicates a that service to be similar enough. Such a replacement of service instantiations is also called re-composition.

4.4 Sharing of Content and Context

Content and context (including sensed information) can be shared from (mobile) sources to multiple (mobile) destinations. Mobility here means that sources, destinations and intermediate nodes can move and be temporarily unavailable. Movements of source and destination may also happen simultaneously.

Realtime content and context have a notion of freshness and priority. In a lot of situations, older data is no longer relevant after a temporal outage or limited available bandwidth, and can be discarded, such as with video broadcast. In other cases, such as cool-chain logistics, the history of context data needs to be recorded but can arrive later.

When the number of destinations increases, unicasting to all destinations will consume more bandwidth and processing power. To overcome this bottleneck, one data stream can be sent towards a group of destinations and be divided there (e.g. multicast). Also for checking who is allowed to get the data, the source may not be able to handle all requests when the number of destinations increases.

The sharing can also be influenced by the destinations, not all destination may require the same rate or selection of information. Therefore, remote configuration is required, in a controlled manner. The configuration of one destination, should not affect the experience of another destination. For instance when a destination requires a context update every 5 minutes, the others can still get it at the default 15 minutes and the source could sent it more frequently towards the first destination. Something similar holds for actuation of the source, destinations can potentially sent conflicting actuation commands, so control is required to determine who has authority and priority to make these changes.

5 Research Challenges and Progress

This section describes research challenges and progress in a number of research projects for realtime mobile sharing of multimedia and WSANs.

5.1 Mobility and Sharing in Heterogeneous Networks

For network mobility we distinguish changes in network attachment of devices[1] (such as mobile phones) and mobile networks (such as a WLAN in the train). A user would typically want to use the network or combination of networks that offers the best cost, bandwidth and latency properties. And when networks are no longer in reach, he/she would rather continue the applications seamlessly than restarting them manually. Moreover, when multiple users are using the same wireless network the user would not like his video stream to be interrupted by less time-critical traffic such as file downloads. The challenge is therefore to offer seamless mobility across heterogeneous networks and efficient sharing of wireless networks such as WLAN.

For optimum use of multiple networks progress has been made in the IST-Daidalos project [4]. For efficient sharing of wireless networks a solution was reported in [34], that shared knowledge on QoS queue-lengths. A recent approach is that of IEEE 802.11e that uses a differentiated scheme with prioritized QoS classes including best-effort, video and audio. IEEE 802.11e also has non-mandatory extensions that can enforce the traffic constraints per terminal and QoS class.

5.2 Mobility and Sharing of WSANs

When a WSAN in a truck or on a body is used by applications over the Internet, it can temporarily lose network connectivity and may have to change to other networks as it moves. These mobility changes have impact on the bandwidth and latency of the information from WSAN, and on the reachability of the WSAN for remote configuration and actuation. Conflicts can arise when multiple applications try to send configuration and actuation commands to the WSAN. Another type of conflicts can arise when WSANs that use the same wireless resources move in each other's coverage area.

---

[1] Note that a mobile device can have multiple network interfaces that can be be connected to different networks simultaneously. Normally applications just use the default network interface, but they can use specific network interface for each connection they make.

Progress has been made in the IST-SENSEI project [18] with a.o. 6LoWPAN [30] and a binary web service protocol. In [14] a middleware solution is presented for sharing WSANs. In [13] approaches for mobility and sharing WSANs are further analysed.

5.3 Mobility and Sharing of Multimedia Sessions

A multimedia session is usually a combination of session control and multimedia streams between endpoints. For multimedia session mobility we therefore distinguish between changes in network interface attachment[1] of session control and multimedia stream endpoints. The latter enables splitting a multimedia session across multiple devices, e.g. move the video from your mobile to a nearby wall display and moving it back later. Multimedia streams can also be shared by multiple recipients when it is multicasted or otherwise duplicated, the challenge is to do this efficiently with realtime content to a dynamically changing and mobile group of users.

Progress has been made in the Freeband 4Gplus project [40] and IST-Daidalos project [3, 4]. A network-initiated method for splitting multimedia sessions is described in [2]. In [47] an approach is described for efficient personalized sharing of multimedia streams.

5.4 Service Platforms

A service platform offers a mobile terminal access to the network and services in heterogeneous networks. Federation between Service Platforms realises a service control layer that extends network and service usage to those of other service platforms. Challenges for service platforms are offering appropriate QoS and security while roaming, sharing your identity across networks and applications and enabling anonymous use of web and multimedia applications.

Regarding progress, mobility schemes for maintaining sessions were analysed in the Freeband 4Gplus project [40] and IST-Daidalos project [3, 4]. The IST-Daidalos project also worked on virtual identities across network and applications, with anonymity support.

5.5 Pervasive Service Platforms

Pervasive service platforms extend service platforms with composition of tailored and context-aware services, streams, context, into an pervasive application. The challenge for pervasive service platforms is to offer adaptability of the pervasive application to all sorts of changes such as environmental, the situation the user is in, the network attachment and the available bandwidth.

Regarding progress, the IST-Daidalos project [3, 4] proposes a pervasive service platform that offers this adaptability. In the context of the IST-Sensei project, a framework was created to enable comparing and combining pervasive communication architectures.

6 Conclusion

In this chapter we have described the main concepts involved in realtime mobile sharing, namely networks, sessions, services, mobility, federated service platforms, sharing and pervasiveness. We have noticed that the combination of these concepts can enable the IoT, IoS and IoM. We have also observed the dynamics of network attachment, multimedia sessions and context and how they can trigger and enable adaptations of pervasive applications. The bottom line is that sharing and mobility are intertwined, and the performance of realtime sharing and mobility handling impacts the efficiency and scalability of pervasive applications. We expect that for efficient realtime mobile sharing, support is required across the mobile device, the network and the service infrastructure.

Acknowledgements. Part of the work described in this chapter are results of the project 4th Generation Platform Launching Ubiquitous Services (4GPLUS), see http://4gplus.freeband.nl, and was supported in part by the Dutch Freeband Impulse Programme on Telecommunication Applications (http://www.freeband.nl) and is co-funded by the Dutch Ministry of Economic Affairs.

Part of the work presented in this chapter was partially funded by the EU project IST-2002-506997 DAIDALOS (Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services), and synthesizes the contributions of multiple project partners.

The work described in this chapter is based on results of IST FP6 Integrated Project DAIDALOS II (IST-2006-026943), which received research funding from the European Communities Sixth Framework Programme.

This chapter describes work in part undertaken in the context of the SENSEI project, Integrating the Physical with the Digital World of the Network of the Future (www.senseiproject.eu). SENSEI is a Large Scale Collaborative Project supported by the European 7th Framework Programme, contract number: 215923.

Apart from the research funding, the European Commission has no responsibility for the content of this chapter. The information in this chapter is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

References

1. 3GPP. IP Multimedia Subsystem (IMS); Stage 2. TS 23.228, 3rd Generation Partnership Project (3GPP)
2. Tuijn, J.A., Bijwaard, D.: Spanning a multimedia session across multiple devices. Bell Labs Technical Journal 12(4), 179–193 (2006)
3. Aguiar, R., Bijwaard, D., Jaehnert, J., Christ, P., Einsiedler, H.: Designing networks for the delivery of advanced flexible personal services: the daidalos approach. In: IST Mobile and Wireless Communication Summit (2004)

4. Aguiar, R.L., Sarma, A., Bijwaard, D., Marchetti, L., Pacyna, P.: Pervasiveness in a competitive multi-operator environment:the daidalos project. IEEE Communications Magazine 45(10), 22–26 (2007)
5. Aguiar, R., Pacyna, P.: Final Daidalos II global architecture. Deliverable DII-124, Daidalos consortium (October 2008)
6. Akyildiz, I.F., McNair, J., Ho, J.S.M., Uzunaliolu, H., Wang, W.: Mobility management in current and future communication networks. IEEE Network Magazine (August 1998)
7. Akyildiz, I.F., McNair, J., Ho, J.S.M., Uzunaliolu, H., Wang, W.: Mobility management in next generation wireless systems. Technical report, Georgia Institute of Technology (1999)
8. Open Mobile Alliance. Common definitions for OMA RESTful Network APIs, OMA-TS-REST_NetAPI_Common-V1_0, `http://www.openmobilealliance.org/` (last visited July 2012)
9. Bargh, M.S., Bijwaard, D., Zandbelt, H., Meeuwissen, E., Peddemors, A.: Mobility management in beyond 3g environments. In: Proceedings of Wireless World Research Forum 9, WWRF 9 (July 2003)
10. Bargh, M.S., Zandbelt, H., Peddemors, A.: Managing mobility in 4g environments with federating service platforms (an overview). In: Proceedings of EVOLUTE Workshop, Evolute 2003 (2003)
11. Berger, A., Romascanu, D.: Power ethernet MIB. RFC 3621, IETF (December 2003)
12. Bhattacharyya, S., Ed, I.: An overview of Source-Specific multicast (SSM). RFC 3569, IETF (July 2003)
13. Bijwaard, D.J.A., Havinga, P.J.M., Eertink, E.H.: Analysis of mobility and sharing of wsns by ip applications. International Journal of Distributed Sensor Networks 2012, 923594 (2011)
14. Bijwaard, D.J.A., Kleunen, W.A.P., Havinga, P.J.M., Kleiboer, L., Bijl, M.J.J.: Industry: Using dynamic WSNs in smart logistics for fruits and pharmacy. In: Proceedings of SenSys 2011, Seattle, WA, USA, November 1-4, pp. 218–231. ACM, New York (2011)
15. Bosch, S., Marin-Perianu, R.S., Havinga, P.J.M., Marin-Perianu, M., Horst, A., Vasilescu, A.: Automatic recognition of object use based on wireless motion sensors. In: International Symposium on Wearable Computers 2010, Seoul, South Korea, USA, pp. 143–150. IEEE Computer Society (2010)
16. BSD. TinyOS, operating system designed for low-power wireless devices, `http://www.tinyos.net`
17. Callas, J., Donnerhacke, L., Finney, H., Shaw, D., Thayer, R.: Openpgp message format. RFC 4880, IETF (November 2007)
18. SENSEI consortium. SENSEI: Integrating the physical with the digital world of the network of the future, `http://sensei-project.eu` (last visited July 2012)
19. Deering, S.: Host extensions for IP multicasting. RFC 1112, IETF (August 1989)
20. Devarapalli, V., Wakikawa, R., Petrescu, A., Thubert, P.: Network mobility (NEMO) basic support protocol. RFC 3963, IETF (January 2005)
21. Dierks, T.: The transport layer security (tls) protocol version 1.2. RFC 5246, IETF (August 2008)
22. Dutta, A., Jain, R., Wong, D., Burns, J., Young, K., Schulzrinne, H.: Multilayered mobility management for survivable network. In: Milcom, Vienna, Virginia (November 2001)
23. Eisenhauer, M., Rosengren, P., Antolin, P.: A development platform for integrating wireless devices and sensors into ambient intelligence systems. In: 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops, SECON Workshops 2009, pp. 1–3 (2009)

24. XMPP Standards Foundation and Google. Xmpp technologies: Jingle, `http://xmpp.org/about-xmpp/technology-overview/jingle/`
25. Freier, A.O., Karlton, P., Kocher, P.C.: The SSL protocol version 3.0, `http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt`
26. Hofmeijer, T.J., Dulman, S.O., Jansen, P.G., Havinga, P.J.M.: AmbientRT - real time system software support for data centric sensor networks. In: Proceedings of the 2004 Intelligent Sensors, Sensor Networks and Information Processing Conference, pp. 61–66. IEEE Computer Society Press (2004)
27. ITU-T. Packet-based multimedia communication systems, `http://www.itu.int/rec/T-REC-H.323/en/`
28. Johnson, D., Perkins, C., Arkko, J.: Mobility support in IPv6. RFC 3775, IETF (June 2004)
29. Kent, S., Seo, K.: Security architecture for the internet protocol. RFC 4301, IETF (December 2005)
30. Kushalnagar, N., Montenegro, G., Schumacher, C.: IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals. RFC 4919, IETF (August 2007)
31. Meratnia, N., van der Zwaag, B.J., van Dijk, H.W., Bijwaard, D., Havinga, P.J.M.: Sensor networks in the low lands. Sensors 10(9), 8504–8525 (2010)
32. Milonas, A.C.: Enterprise networking for the new millenium. Bell Labs Technical Journal 5(1), 73–94 (2000)
33. Misra, A., Das, S., Agrawal, P.: Application-centric analysis of IP-based mobility management techniques. Journal of Wireless Communications and Mobile Computing 1(3) (August 2001)
34. Peelen, B., Zivkovic, M., Bijwaard, D., Teunissen, H.: Supporting qos in broadband wireless and wired access. Bell Labs Technical Journal 8(2), 65–81 (2003)
35. Perkins, C.: IP mobility support for IPv4. RFC 5944, IETF (November 2010) (revised)
36. Perkins, C.: IP mobility support for IPv4. RFC 3344, IETF (August 2002)
37. Perkins, C., Johnson, D.B.: Mobility support in IPv6. In: Second Annual ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom 1996, pp. 27–37 (1996)
38. Politis, C., Chew, K.A., Tafaz, R.: Multilayer mobility management for all-IP networks: Pure SIP vs. hybrid SIP/mobile IP. In: The 57th IEEE Semiannual Vehicular Technology Conference, VTC 2003-Spring (2003)
39. Roach, A.: Session initiation protocol (SIP)-Specific event notification. RFC 3265, IETF (June 2002)
40. Romijn, W.A., Plas, D.-J., Bijwaard, D., Meeuwissen, E., van Ooijen, G.: Mobility management for SIP sessions in a heterogeneous network environment. Bell Labs Technical Journal 9(3), 237–253 (2004)
41. Rosenberg, J., Schulzrinne, H.: Session initiation protocol (SIP): locating SIP servers. RFC 3263, IETF (June 2002)
42. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: SIP: session initiation protocol. RFC 3261, IETF (June 2002)
43. Saint-Andre, P.: Extensible messaging and presence protocol (XMPP): core. RFC 3920, IETF (October 2004)
44. Schulzrinne, H., Rao, A., Lanphier, R.: Real time streaming protocol (RTSP). RFC 2326, IETF (April 1998)
45. Schulzrinne, H., Wedlund, E.: Application-Layer mobility using SIP. Mobile Computing and Communications Review (MC2R) 4(3), 47–57 (2000)

46. Stewart, R.: Stream control transmission protocol. RFC 4960, IETF (September 2007)
47. van der Gaast, S., Bijwaard, D.: Efficiency of personalized content distribution. Bell Labs Technical Journal 13(2), 135–145 (2008)
48. van Eijk, R., Brok, J., van Bemmel, J., Busropan, B.: Access network selection in a 4G environment and the roles of terminal and service platform. In: Proc. of Wireless World Research Forum 10, WWRF 10 (2003)
49. Wedlund, E., Schulzrinne, H.: Mobility support using SIP. In: 2nd ACM/IEEE International Conference on Wireless and Mobile Multimedia (WoWMoM), Seattle, Washington (August 1999)
50. Jingle session transfer, `http://xmpp.org/extensions/xep-0251.html` (last visited July 2012)