The Mobile VCE Architecture for the Interworking of Mobile and Broadcast Networks

Paul Pangalos[1], Kar Ann Chew[2], Nima Sattari[1]
Allan Tomlinson[3], Robert Atkinson[4], Hamid Aghvami[1] Rahim Tafazolli[2]

[1]King's College London, University of London, 26-29 Drury Lane, London WC2B 5RL
[2]University of Surrey, Guildford, Surrey GU4 7RB, UK
[3]Royal Holloway, University of London, Surrey TW20 0EX
[4]University Of Strathclyde, Glasgow G1 1XW, Scotland

Abstract: The Core 3 Research Programme of the Virtual Centre of Excellence in Mobile and Personal Communications (Mobile VCE Core3) takes a generic approach for the co-operation between mobile and broadcasting network, such that the solution is more widely applicable and easily adopted by network operators, service providers and customer owners. This also reflects the industrial reality of the competitiveness that exists between the broadcast and telecommunications industry – both believe in convergence. This paper presents and describes the low level functional elements of the inter-working of networks Mobile VCE architecture. In particular, it focuses on the network components and briefly describes the structure and key functionalities of three of them namely mobility management, security and the personal distributed environment.

Introduction

The co-operation between mobile and broadcasting in MVCE Core 3 Research Programme is based upon the principle of interworking as distinct from integration of networks which implies a transfer of network control. A distributed and non-uniform intelligence across the inter-network architecture is assumed. Each network is an administrative domain inter-working and co-operating with each other to provider a better service to their users, but they are owned by and under control of their respective operator ,. The access networks are inter-connected via a logical interface enabling inter-working at the network and service layers.

Figure 1 gives a summary of the baseline architecture proposed for consideration within MVCE Interworking of Network (IoN) Work Area. This architecture does not suggest any alteration to the existing network architecture, other than creating interfaces among the networks involved.

Interworking-related signalling between networks is carried out over the entity known as IoN Gateway (IGW) residing in each network. An IGW represents an administration domain and communicates with IGW of another domain to which an interworking agreement has been established. IGWs are interconnected via logical channels known as the IoN Link.

This interface enables signalling and information exchange for the vertical handover purposes. The logical connection between two gateways is provided by an underlying transport network with certain bandwidth and other quality of service (QoS) guarantees. IGW is also the gateway that allows service and content providers to exploit interworking of mobile and broadcasting networks. It provides the interface for any service/content provider who wants to provide service/content over both mobile and broadcasting networks. Therefore, IGW is the signalling gateway between networks and network as well as service gateway between network and service provider.

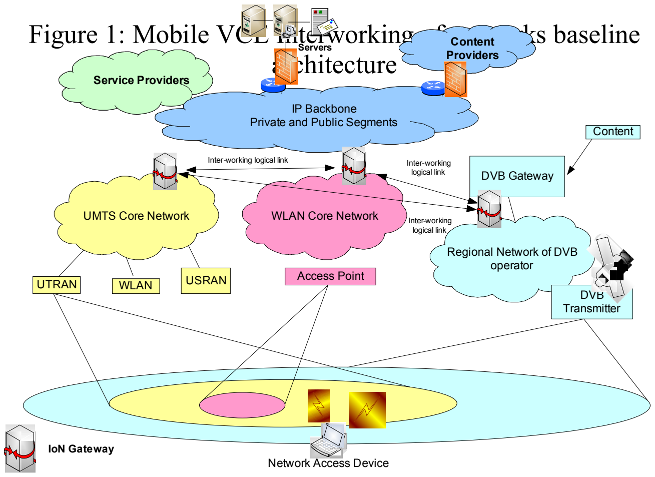


Figure 1: Mobile VCE Interworking of Networks baseline architecture

Adopted Business model

IoN adopts an incremental and evolutionary approach to mobility management by enhancing existing solutions to vertical handovers based on existing business models. The current cellular business model is operator centric illustrated in Figure 2. This means the network operator has telecom as their core business and oriented towards filling the network with traffic and earning money on mobile services only. In this model, each user has an initial subscription with the so called home network and uses standard network specific procedures and parameters for authentication. The network operator maintains a subscriber database containing the profiles and all user service related definitions. In addition, this model provides integrated robust authentication and billing mechanisms as well as rigid security features that establish an important level of trust between the operators and its subscribers .

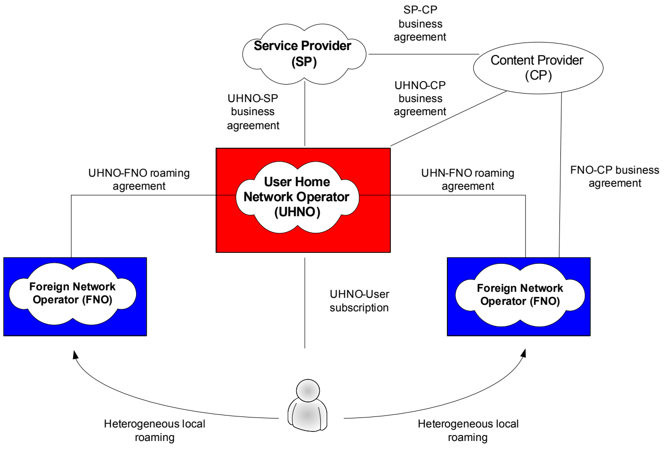

SP-CP business agreement
Service Provider (SP)
Content Provider (CP)
UHNO-SP business agreement
UHNO-CP business agreement
UHNO-FNO roaming agreement
User Home Network Operator (UHNO)
UHN-FNO roaming agreement
FNO-CP business agreement
Foreign Network Operator (FNO)
UHNO-User subscription
Foreign Network Operator (FNO)
Heterogeneous local roaming
Heterogeneous local roaming

Figure 2: Traditional Business Model

low level Architecture

The overall aim of the Interworking of Networks (IoN) activity is to investigate and define interworking procedures between cellular-based mobile networks, WLAN and digital broadcasting networks. The main objective for the IoN architecture is to develop technical solutions to allow seamless provision of a suite of services, ranging from entertainment to e-business, to both individuals and group of users, which can only be supported, or can be supported more cost-effectively, by jointly leveraging assets of all the networks together. To carry this out, the following architecture components were developed as shown in Figure 3.

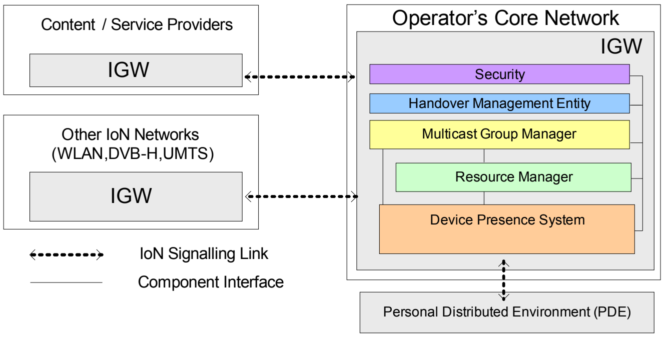


Figure 3: IoN network architecture components

Mobility Management

Within this research work, it is assumed that a collection of terminals are connected to an IoN mobile router (IMR). The IMR is assumed to have the multimode capability of connecting to both mobile and DVB networks. It acts as an intermediary or bridge for devices that cannot connect directly. For instance, IMR could be one and the only terminal in a train that is equipped DVB hardware for proper broadcasting reception, other terminals onboard could exploit IMR's capability for receiving data broadcasted by DVB network. Similarly, IMR can be a terminal which is part of a user's a personal area network and is bridging all user's devices to the mobile and broadcasting networks. One of the major functions of IMR is support the mobility and handover of the group of terminals connected to it. The collective of terminals, together with the IMR, form a network and move as a single unity. IMR performs vertical handovers to support the network, and all terminals associated with it, moving across mobile and broadcasting networks. Vertical handovers are more complicated than horizontal ones and require careful consideration and understanding in order to make the transition transparent to the user , .

A new entity is introduced located within the DVB and mobile networks that is responsible for handover management and deals with issues such as: monitoring of traffic, exchanging the relevant signalling information necessary for handover and triggering/executing handovers. This entity is also referred to as the handover management entity (HME) and represents all the necessary operations that are required in order to initiate and complete the handover. Some of these functions will be carried out by other existing entities in the mobile networks and some in the DVB. The handover is carried out in three phases: initiation phase, execution phase and completion phase.

Handover initiation: One of the responsibilities of the handover entity is monitoring and triggering the handover. Consider a train at a railway station. The train's connectivity to the outside world is provided by its IMR, and the train's WLAN network provides connectivity to the IMR for all users in the train. As long as the train is in the station, the IMR stays connected to the station's WLAN hot spot because it provides high bandwidth at low cost. Hence the station's WLAN network provides the necessary connections for users in the train via the train's IMR. As the train departs from the station, it gradually leaves the coverage area of the station's WLAN network. In order to maintain users' current services without interrupting connections, users should be handed over to an available DVB access network before the WLAN coverage is lost. Discovering the right time to perform a handover is a key issue. Only though prompt reactions can a handover be initiated and performed efficiently. In order to predict the correct time to perform the handover, the handover management entity uses the concept of the "Handover Initiation Time (HIT)". By using the HIT concept, the IMR can ensure that the handover will be completed before the train leaves the station's WLAN coverage area, and guarantee (in most cases) that users maintain sufficient QoS throughout the process. As a result of this scheme, the handover process reduces packet loss and handover performance. Furthermore, a very important part of this phase is the algorithm that decides which return channel is used.

Handover Execution: In this phase, the handover entity requests for the other networks resource availability information as well as cost for the particular traffic class/service. Once this information is obtained a handover procedure is executed. This procedure allows uninterrupted session support by using two or more simultaneously active interfaces at the IMR. The handover management entity uses an extended version of Mobile IP to execute the handover. Mobile IP provides the network layer of the HME with smart routing and proxy filtering decisions being taken at the home agent. The HME has an update profile of its registered IMRs and provides filtering according to selected interface and user sessions. Once a user hands over to a different type of network the routes are updated dynamically by Mobile IP. The IP packets are then intercepted, processed and filtered transparently to the user and sent from the home agent to the mobile host.

Handover completion: Once the handover is executed, the HME is responsible for clearing any previous tunnels and updating other entities within the IoN architecture.

Security

Full inter-networking between mobile, broadcast network requires security functionality at different positions. Most mobile and broadcast networks already have existing security facilities which rely on a relationship between network operator, content provider and the end users. With interworking, content can be provided using a mix of broadcast and mobile networks, each with different mechanisms for content protection and different payment models. Users of such networks need to establish a security context, yet will not want separate tokens for each network or service accessed. The implementation of interworking to support enriched services requires security mechanisms which are robust but also simple, indeed transparent, to the user, if the requirement of ease-of-use is to be achieved. Furthermore, the existing security mechanisms need to be supported.

Threats and Security Requirements

Several networks may interact to provide services to the user. In this model the user may access the same content via several different terminals and different routes, depending on the location and which terminal is being used. The threats to such model are summarised in Table 1.

Network Services	Threats
Confidentiality and integrity of messages, and authenticity of sources	Illegitimate use of networks and services; information leakage; integrity violation; denial of service.
Secure handover	Illegitimate use of networks, services, or communication sessions.
Secure means of informing users and networks of changes in delivery mechanism and presenting options	Integrity violation Denial of service
Diversity of authentication mechanisms for different service providers.	Denial of service Illegitimate use of service
Connecting to external networks. An authentication service to provide mutual network to network authentication.	Threat to both the network and the user: illegitimate use
Privacy of financial transactions	Information leakage
Confidentiality of user profiles	Information that identifies users should not be transferred across networks.
Protection from subliminal data leaks, such as gathering information from traffic analysis	Information leakage

Table 1: Summary of Threats in IoN

To address these threats, the following security services should be provided by the IoN security architecture: Mutual Authentication; Single Sign-On; Protection, revocation, and renewal of credentials; Interoperability with local security solutions; Mechanism independence; Delegation; Privacy; Confidentiality; Integrity; Policy Exchange; and Secure Logging. This is discussed in more detail in and .

Based on the above, several requirements are identified. One requirement is to enable access to mobile and broadcast networks without separate security tokens (SIMs, smart cards, etc.) and agreements. A second requirement is to enable secure content-based transactions between content provider, mobile and broadcast network operators, and consumers. This requires secure information transfer for billing, quality and usage metrics, and security provision for service delivery in mobile and broadcast networks. Information exchange between network operators themselves must also be secure, to ensure that interworking service agreements are not violated. Therefore, two aspects of security are being addressed. One concerns transactions, between users and networks. The second is security between networks.

The overriding security concern is that of authentication. Unless the authenticity of both entities in a security context is established it will be difficult to meet any of the other requirements. Therefore, the research effort for security for interworking of networks is initially focussing on authentication. In addition to the fundamental security requirements identified above, interworking of networks introduces new issues arise with the potential delivery of broadcast services to mobile terminals; content protection under interworking system is also a major concern . The following section presents some of the initial outcomes that addresses the issues on authentication and content protection.

Authentication

To establish a security context, both entities have to exchange and verify credentials.   In an open architecture, many separate security domains exist, each using their own security mechanisms and managing their own security policies. The challenge, then, is to negotiate a set of common security mechanisms and policies that both parties can agree on and support. Once this is accomplished, credentials can be exchanged, authenticity verified, and the security context established.

This challenge is not unique to the interworking of mobile and broadcasting networks. The provision of services over the Internet also requires the same mutual authentication between security domains in an open system. Consequently, standards that have the potential to address this problem are now emerging. The Web Services architecture includes a security framework, WS-Security that allows entities to construct and exchange secure XML based SOAP messages. This provides an extensible framework that security of network and services could be based on. Figure 4 illustrates how the concepts of WS-Security can be applied to authenticate and establish a security context in interworking of networks.

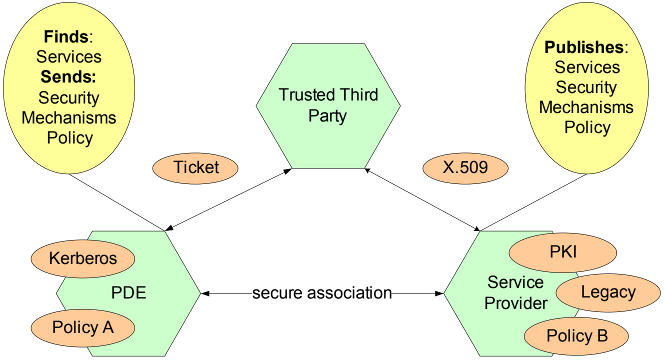
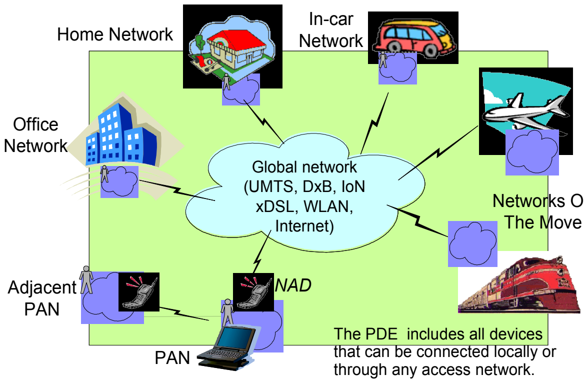


Figure 4: Establishing a security context

Interaction with User's Personal Network

Within the Mobile VCE Core 3 research programme, much work is also being carried out on a Personal Network (PN) solution known as the Personal Distributed Environment (PDE) . The PDE is a user-centric approach for communication in which users are offered the ability to access services from different sources, using different devices, via heterogeneous access networks and under different conditions in a transparent way. Devices in immediate vicinity of the user form a self-organising Personal Area Network (PAN), however the user's PDE is not merely a physical PAN but a virtual personal network. The user's PAN is extended to remote devices using external data delivery mechanisms including fixed, mobile and broadcast network through a gateway terminal known as a network access devices (NAD). The NAD connects the user's PAN, and hence the PDE to the outside world. A representation of the PDE is given in Figure 5.



Home Network
In-car Network
Office Network
Global network (UMTS, DxB, IoN xDSL, WLAN, Internet)
Networks On The Move
Adjacent PAN
NAD
PAN
The PDE includes all devices that can be connected locally or through any access network.

Figure 5: The concept of a personal distributed environment

In the following description, the term PDE refers to the personal network concept developed in the Mobile VCE as well as the Work Area within the Mobile VCE (also known as PDE) that carries out research on this concept.

The PDE focuses upon the challenges of user's individual communication environment and enriched service delivery. Service delivery involves not only user's terminals but various networks that set up the communication paths. Neither the user's short-range wireless terminals nor the networks alone are able to provide such a service environment. Therefore, a close interaction between the PN and interworking networks, particularly at the service and network level, is essential. Indeed, the interworking of networks complement user's personal network to enable the enriched and user-centric service. For example, resource and group managements in the networks support efficient service provision by identifying of the most suitable delivery mode (e.g. multicast, broadcast; via mobile or DVB network); whereas service support within user's personal network take a user-centric view in network selection based on the user's preferences, purpose of communication, terminal capability, quality of short range radio connection between terminals etc. While the interworking system is primarily concerned with a single multimode terminal, the user's personal network is concerned with service provision within a range of terminals, each with its own communication and processing capability. It considers an added dimension to the problem space by investigating network selection across the multiple terminals at the disposal of user personal network. In order to make effective decision on which network-terminal pair is the most suitable for a particular service, the user's personal network need to interact with networks and vice versa.

CONCLUSIONS AND FUTURE WORK

The co-operation of mobile and broadcasting networks is based upon the principle of interworking rather than integration. Based on this principle, networks are not being merged but remain autonomous and independently-managed domain. Various tools and solutions required to enable effective interworking between operators, as well as interactions between users and networks, are investigated by this research activity. Other topics being addressed include:

- A novel group management for multicast and broadcast-based service that aims to develop interworking extensions for MBMS and the DVB-T/H networks. The multicast group manager provides a mechanism for setting up and transferring multicast-based data from one network to another.
- A distributed resource management framework that monitors resources across the networks and provides the most efficient (from a cost point of view) network to use for a given service . This also includes the possibility of sharing resources between networks.
- The device presence system (DPS) provides discovery, management and tracking of user devices within an IoN environment. It enables the network to maintain up to date information related to all the network access devices under the user's control as well as context information required to initiate IoN services.

The current and future research effort is focusing upon the interaction and signalling procedure among all the functional blocks addressed in this paper. While all of the functional entities have been developed on modular basis, the interactions and necessary signalling among them are also being identified.

ACKNOWLEDGEMENT

The work reported in this paper has formed part of the work area 5 of the Core 3 Research Programme of the Virtual Centre of Excellence in Mobile & Personal Communications, Mobile VCE, www.mobilevce.co.uk, whose funding support, is gratefully acknowledged. More detailed technical reports on this research are available to Industrial Members of Mobile VCE.

REFERENCES

[1] Pangalos, P., Chew, K., and Aghvami, H., "Inter-working aspects between 3G and Digital Broadcast Networks" WWRF11, 10 - 11 June 2004, Oslo, Norway

[2] Pangalos, P., Morris, D., Sattari, N., Aghvami, H., Chew, K. and Tafazolli, R., "Inter-working of Broadcast, WLAN and Cellular networks", WWRF9, Zürich, Switzerland, 1-2 July 2003.

[3] Sarraf, C., "MVNOs – The 'New' Concept for Mobile Operators", Ericsson Lebanon

[4] Sattari, N., Pangalos, P. and Aghvami, H., "Handovers between UMTS and WLAN" VTC2004, Italy Milan, May 19-21, 2004.

[5] Sattari, N., Pangalos, P. and Aghvami, H., "Handover among Heterogeneous Networks using NEMO", WWRF12, 4-5 November 2004, Toronto, Canada

[6] Schwiderski-Grosche, S., Tomlinson, A., Irvine, J. M., Goo, S. K. "Security challenges in the Personal Distributed Environment" in proc. VTC Fall '04, Los Angeles, USA, IEEE, October 2004.

[7] Tomlinson, A. and Schwiderski-Grosche, S., "Application of Grid Security to Personal Distributed Environments", in proc. GADA'04, Cyprus, Springer-Verlag LNCS, Oct. 2004.

[8]Dent, A. and Tomlinson, A., “Regional Blackouts: Protection of Broadcast Content on 3G Networks”, in proc. Fifth IEE International Conference on 3G Mobile Communication Technologies (3G 2004), London, October 2004.

[9]Gallery, E., and Tomlinson, A., “Conditional Access in Mobile Systems: Securing the Application” ” in proc. DFMA’05, Besançon, France, IEEE, to appear Feb. 2005.

[10]Dunlop, J., Atkinson, R., Irvine, J. and Pearce, D., “A Personal Distributed Environment for Future Mobile Systems” IST 2003, Aviero, Portugal, June 2003.

[11]Huang, L., Chew, K., Tafazolli, R., “Distributed Resource Management for Interworking of Cellular and Digital Broadcasting Networks,” IST Mobile Summit, June 2004.