PERIMETER: Privacy-Preserving Contract-less, User Centric, Seamless Roaming for Always Best Connected Future Internet[1]

Frances Cleary, Waterford Institute Of Technology, Ireland

Markus Fiedler, Blekinge Institute of Technology, Sweden

Lenny Ridel, Traffix Systems Ltd., Israel

Ahmet C. Toker, Technische Universität Berlin/DAI Labor, Germany

Barış Yavuz, Turkcell Iletişim Hizmetleri A.Ş., Turkey

Abstract— **PERIMETER is a new EU FP7 project, whose main objective is to establish a new paradigm of user-centricity for advanced networking. In contrast to network-centric approaches, user-centric strategies could achieve true seamless mobility. Putting the user at the centre rather than the operator enables the user to control his or her identity, preferences and credentials, and so seamless mobility is streamlined, enabling mobile users to be "Always Best Connected" in multiple-access multiple-operator networks of the Future Internet.**

For this purpose, PERIMETER will develop and implement protocols designed to cope with increased scale, complexity, mobility and requirements for privacy, security, resilience and transparency of the Future Internet. These include appropriate mechanisms for network selection based on Quality of Experience; innovative implementation of "Distributed A3M" protocols for Fast Authentication, Authorisation and Accounting based on privacy-preserving digital identity models. All these mechanisms will be designed to be independent from the underlying networking technology and service provider, so that fast, inter-technology handovers will be possible.

Index Terms—**Future Internet, Quality of Experience, Privacy, Trust**

I. INTRODUCTION

The realization of a user-centric paradigm for seamless mobility, which implies a free and automatic choice between different available wireless and mobile access networks in an Always Best Connected manner [1], will revolutionize the Future Internet. To work towards the materialization of this innovative concept a paradigm shift is required from contract-based mobile service delivery, that limits the ability of the user to choose the best provider for the needed service, to a dynamic, contract-less service delivery based on privacy-preserving identity management [5] and employing a proxy billing service, analogous to Pay-Pal [4] service for online payments. Within the PERIMETER research project the basis for the user-centric paradigm will be established. This involves taking into account distributed and highly scalable mechanisms for trust, reputation and authorization required for fast handover and unified billing. Through concentrating on other key concepts such as QoE model definitions and measurements this in turn will progress the work in the handover triggering and content adaptation, which significantly extends earlier work on this topic such as [2], [3]

[1] This research activity is funded under the EU ICT FP7 project, PERIMETER (Project No.: 224024).

II. YESTERDAY, TODAY, AND PERIMETER

A. Network Centricity vs. User Centricity

Figure 1 illustrates the network- (and thus operator-) centric view that has been adopted so far. Figure 2 conveys a potential future view the operational aspect of having the user at the centre promoting the paradigm shift from previous operator/network-centric approaches towards a user-centric approach that the PERIMETER project will address and impact.

B. PERIMETER Architecture

The main pillars of the PERIMETER architecture are the QoE model associated with different applications running on the user equipments, a peer-to-peer overlay in which the users and selected nodes in the access network are members, and a privacy-preserving fast AAA mechanism. A middleware running on the user equipment is responsible for gathering information from the device, usage and network context to fill the parameters of the QoE model. This information is distributed among the peers in the overlay network, using a trust mechanism embedded in the middleware. Based on local perception of QoE, and information from trusted nodes the middleware distributes the flows of different applications to different access technologies. The decision mechanism maximizes the perceived QoE within the boundaries set by user preferences, defined as policies. The fast AAA mechanism is responsible for establishing privacy-preserving associations with different access networks, which is valid for the lifetime of the session.

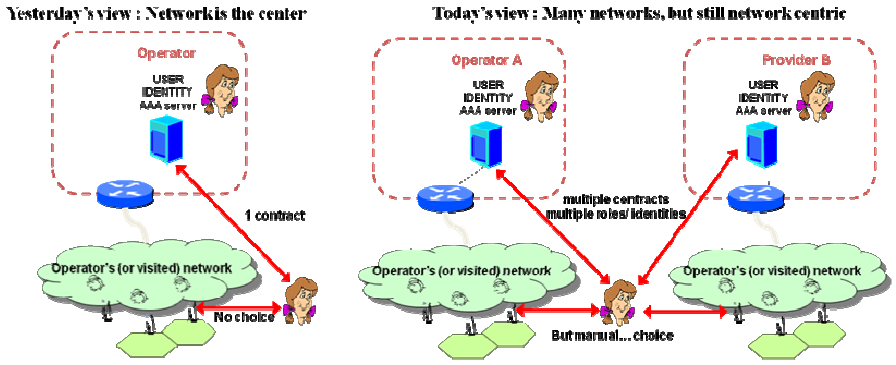

Fig. 1 Network Centric view of yesterday and tomorrow

The PERIMETER project pushes these boundaries through the design and development of user-centric privacy and anonymization mechanisms, that will allow end users to enjoy privacy protection and if required, logically separate their identity and their activities on the network from the billing process, while retaining their ability to autonomously select the best connection and best service from the available choices in each area. These mechanisms will be designed to be independent from the underlying networking technology, so that fast, inter-technology handovers will still be possible.

Through this innovative architecture, PERIMETER will progress deployment of heterogeneous multi-access-technology/operator based system, that will demonstrate the concepts dynamic, contract-less roaming and privacy-preserving identity management and unified billing.

By facilitating a unified billing approach this allows end users access to different networks of different operators. This innovative billing aspect that is being adopted by PERIMETER, will actively encourage the access network providers and the service providers to provide support for such a flexible billing and business model. This paper will highlight the aspects of the PERIMETER middleware that will work towards the implementation of such innovative unified billing models all the while taking into consideration the privacy aspects of such a system in order to limit any unnecessary data disclosure that could be detrimental to the end user.

PERIMETER will undoubtedly work towards the empowerment of the end user, providing them with the added ability of being capable of protecting their end user personal information data, it will also ease the overall billing process the end user has with the various network providers, which will work towards providing a secure, user friendly and seamless mobility option for today's network end users.

C. *Adaptation Models*

As with any considerable technological innovation, which we expect to achieve in the end of PERIMETER, there are two paths for wide acceptance of the innovation, evolutionary and revolutionary. Contrary to the revolutions in the history, this revolution would have to be done by the regulators – the European governments – by changing the regulations, and allowing the dynamic contracts we are proposing. This is analogous to the number portability, where operators are forced to let go of their privileges – and financial benefits associated with these – since there is a considerable benefit for the users, who are represented by their governments.

Even if we argue for a revolutionary deployment, there has to be proof of concept deployments before the actual deployment that happens after regulation change.

To this end PERIMETER project will adopt the Living Lab concept by using few reference scenarios and a small users population, that may be interested in using multiple providers and reserving some unused bandwidth for these users; business travelers, or cross-border workers are interesting groups. The scenarios highlight the following innovative PERIMETER concepts, to be incorporated and displayed in the final PERIMETER demonstrator.

D. *Demonstrative Scenarios*

Scenario 1: The first scenario considers an always best connected user that roams between different technologies and operators. We denote this scenario as "agnostic ubiquitous communication", referring in particular to the need of users to be connected according to their specific needs irrespective of the technology, service provider, devices and media available.

Several solutions have already been proposed to ease handovers with respect to particular access technologies and transport protocols: inter-access-technology handovers of VoIP phone calls from UMTS to IEEE 802.x networks have been successfully demonstrated [7], [8]. There are a number of few important questions that deserve further analysis: one regards what the user experiences when handovers occur and how the handover can be transformed from a technological solution to provide mobility to a mechanism to enhance the user's quality of experience. Reaching this objective requires the focus of mobile networks to shift from applications, devices, or protocols that are playing, generating or transmitting data to the interaction between the user and the data itself and how this interaction is influenced by handovers. From the point of view of the user, a video-call run on a mobile phone is just a medium to keep in touch with a remote colleague or friend: the user only cares about the real time audio-video signals, no matter how these are collected from the network and ultimately by which device they are played. The same applies to all those activities that involve transmission of data over a network such as on-line gaming, file sharing, web-surfing and so on: switching of involved devices, applications and technologies should hence happen to improve the user's experience with low user intervention or with no knowledge at all (seamless

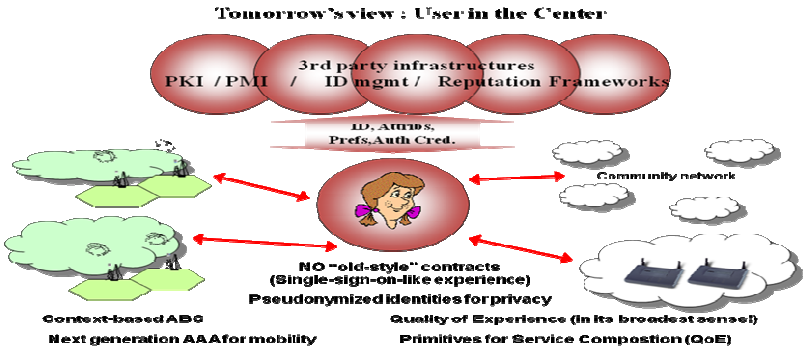

Fig. 2User Centric networking paradigm

switching).

A critical key to this new approach requires a handover framework under the almost complete control of the users, rather than the operators. For example, the user must retain the right to decide how (e.g., under which economic, technological, social conditions) and when [inter-technology] handovers should occur when particular conditions are met. Of course the user should be able to express this control not directly by mingling with network interfaces, direct measurement or assessment of QoS and QoE parameters and so on. The networking infrastructure should be able to collect network and user-level statistics and status variables, process them, and perform handovers and network changes autonomously under the rules set by the users, even dynamically, through specific QoE policies that are controllable by the users, with the highest level of transparency possible.

This approach should be applicable not only to network connections per-se: even the application itself and the device running the application should be switchable in a seamless way. For example, an on-line game can be moved from a mobile phone to a laptop and undergo a technology switch from UMTS to WLAN. After the handover, however, users data such as score and position in the virtual world do not change. Similarly video/voice calls, on-line games, file transfers and so on should be identified by their session data that is independent of the access technology that is used at a particular time, the current application that is running the session data and the device used by the player.

Finally, the protocols that transport user data must be taken into consideration when dealing with this extended handover concept. This is especially important when dealing with device and application switching, for example when moving a telephone call from VoIP to a GSM phone. It is worth noting that during these types of session handovers the format of the transmitted data can change, e.g., to cope with a bit-rate change.

Scenario 2: The second scenario is concerned with the use of the wireless Internet in case of emergency management or in case of a particular health monitoring application where connectivity is critical for the running application.

In a situation of emergency the possibility to communicate is mission-critical. So far organizations that need extremely reliable telecommunication infrastructures usually end up deploying their own networks. For this reason there are technological solutions designed for being used by government agencies, and emergency services, such police forces, fire departments, ambulance, rail transportation staff, transport services and the military. Networks deployed by these organizations usually do not interconnect to each other, without any cooperation they fall in different administrative domains. Network management functions are then replicated in every domain, introducing a substantial waste of monetary, human and technological resources. While the high cost itself might be an acceptable drawback to deploying private infrastructures for critical needs, other functional problems of this un-integrated approach to emergency communication services require further research [9], and are at the center of this use case.

In case a terminal moves out of the coverage of the network, no handover is possible to gain connectivity by other network technology, because emergency service networks are usually neither connected to other networks nor to the public Internet. The Internet of the future should be able to assist emergency services merging them in a single backbone together with other types of traffic, but still assuring the priority, QoS, security and reliability that are expected for this kind of services. Furthermore QoE and QoS-aware wireless Internet should be able to support advanced types of social services that go beyond emergency situations. There are networks applications for the citizens that aim to improve life quality that nowadays do not have proper networking support. For example, the monitoring of patients with critical hearth defects is now performed almost exclusively within hospitals, forcing patients to abandon any hope of a normal life to be constantly monitored inside the hospital. The adoption of online monitoring devices exploiting the PERIMETER middleware for a reliable and secure connection is an innovation that would improve the quality of life of this and other types of patients.

This latter application can be seen as a particular case of the more generic scenario depicted in the previous section. However in this case the QoS, privacy and reliability aspects take a much stronger focus rather than the issues related to multi-device, multi-protocol handovers. With this caveat, some of the requirements stemming from the analysis of these two cases will be inter-related and, sometimes, overlapping.

Scenario 3: The third scenario takes into consideration innovative models of Internet access, where the traditional approach user to ISP is extended to other players that can provide Internet access with different business models.

Around the year 2000 WiFi hardware was cheaply available on the market. This technology encountered a very big success, and as soon it was embedded in every laptop, it spread widely practically everywhere from business sites to private homes.

New business models appeared due to WiFi: ISPs started to deploy 802.11 Access Points (AP) in strategic sites (Hotspots) to offer Internet access. Today the WiFi is so common that most places in urban areas are covered by the signal of some access point, and wireless Internet connectivity is a standard service in most Airports, Train Stations, Public Libraries, Hotels, Restaurants and Coffee Shops.

Wireless "hotspots" are not the only source of public Internet access available. The awareness of security threats at the beginning of the WiFi boom was little, so that individuals and minor organization would leave their network open and serve free and anonymous Internet access to the people nearby. This was the easiest way for little business in public places (such as bars and restaurant) to give free Internet access to their customers and make their place more attractive than others.

Due to the boom of the phenomenon on one side, and political events on the global scale that tended to increase public awareness against misuse of telecommunication infrastructures, many European countries introduce stricter rules on Internet access forbidding the explicit sharing of Internet access. ISPs came into play, proposing in touristic and business places their own access solution with proper access authentication compliant with emerging laws.

Still, in large residential and urban areas it is usually common to find some open network to connect to the Internet, most of the time APs left open by less technology-savvy users that left their network without protections.

These solutions are not based on a common standard, and every single HotSpot follows its own implementation dependent architecture, even if most of the solutions are based on Captive portal authentication with backend RADIUS servers.

Despite regulations some no profit organizations ran by volunteers continued to install WiFi networks to interconnect people and provide free and anonymous Internet access. This is the case of the Wireless Communities, a phenomenon started in the year 2000 and now present in most cities in Europe. These communities built local open network infrastructures in the cities where they are present (Vienna, Roma, Berlin, Luxembourg) with cutting edge wireless mesh network technologies.

Furthermore, many townships in Europe have recently started, or have already completed, projects to offer WiFi services to both citizens and tourists, either for free or subject to very small service fees.

Overall, WiFi networks in European cities are extremely common, and the ensemble of these networks provides a capillary geographical coverage. This big access infrastructure is not yet exploited. The PERIMETER middleware will provide proper access control and handover mechanisms to let the user exploit all the available bandwidth offered with proper security and access control.

These scenarios in turn will be evaluated and assessed in order to successfully analyze the new PERIMETER paradigm usability and applicability of QoE-based user-centric seamless mobility.

E. Conclusion and Future Work

As of the writing of the paper, the partners involved in the project hve finalized the technical specification of the PERIMETER architecture, and have begun with the implementation of the main components. Following a spiral development cycle, three demonstrators of increasing functionality will be implemented, each concerned with the three demonstrative scenarios described above. User centricity will also be incorporated during the development and testing cycle, by employing the Living Lab approach.

ACKNOWLEDGMENT

The authors thank the colleagues working in the following partners of the PERIMETER project: University of Geneva, Fachhochschule Vorarlberg GmbH, Consorzio Nazionale Interuniversitario per le Telecomunicazioni, Telefonica I+D, Grupo Corporativo GFI Informática.

REFERENCES

[1] L. Isaksson. Seamless Communications: Seamless Handover Between Wireless and Cellular Networks with Focus on Always Best Connected. Ph.D. Thesis 2007:06. Blekinge Institute of Technology, ISBN: 978-91-7295-079-9, March 2007.

[2] M. Fiedler, S. Chevul, L. Isaksson, P. Lindberg, and J. Karlsson. Generic communication requirements of ITS-related mobile services as basis for seamless communications. Proceedings of NGI 2005, Rome, Italy, April 2005.

[3] S. Chevul, L. Isaksson, M. Fiedler, P. Lindberg, and R. Waltersson. Network Selection Box: An Implementation of Seamless Communication. 3rd EuroNGI Workshop IA.8.3 Workshop on Wireless and Mobility, Sitges, Spain, June 2006. Springer Verlag, LNCS 4396: Wireless systems and Mobility in Next Generation Internet.

[4] PayPal Home Page: http://www.paypal.com

[5] ITU-T Report on "Identity Management Framework for Global Interoperability", International Telecommunication Union, 2007.

[6] Higgins Home Page: http://www.eclipse.org/higgins/

[7] J. Latvakoski, P. Valitalo, T. Vaisanen, "Vertical handover during a VoIP call in hybrid mobile ad hoc networks", Wireless Telecommunications Symposium, 2008 (WTS 2008), Pomona, CA, 24-26 April 2008

[8] S. Salsano, C. Mingardi, S. Niccolini, A. Polidoro, L. Veltri, "SIP-based Mobility Management in Next Generation Networks", IEEE Wireless Communication, Vol. 15, Issue 2, April 2008, Page(s): 92-99

[9] "TErrestrial Trunked RAdio (TETRA)", European Telecommunication Standards Institute (ETSI), http://www.etsi.org/WebSite/Technologies/TETRA.aspx