A New Perspective on Mobility Management Scenarios and Approaches

Tiago Condeixa[1], Ricardo Matos[1], Alfredo Matos[1],
Susana Sargento[1], and Rute Sofia[2]

[1] Instituto de Telecomunicacões, University of Aveiro, Portugal
{tscondeixa,ricardo.matos,alfredo.matos,susana}@ua.pt
[2] IAN, UTM, INESC Porto, Porto, Portugal
rsofia@inescporto.pt

Abstract. Currently and in the future, users demand for ubiquitous network connection to interact with the world. Moreover, the mobile devices are increasingly widespread and are better equipped in terms of access connections and services support. Mobility management is therefore an intrinsic feature of mobile networks; however, it is not yet ready to support the so called User-provided networks (UPNs), where the network elements can be devices controlled by regular users, or providers, and share subscribed access. In these scenarios, mobility has to be rethought to consider user-centric approaches. This paper discusses the efficiency and applicability of current mobility assumptions in user-centric scenarios, discussing their requirements and solutions addressing several types of networks that may exhibit user-centric characteristics. It also identifies the fundamentals of a user-centric mobility management architecture able to efficiently deal with the dynamicity of the aforementioned scenarios.

Keywords: mobility management, user-centric, scenarios, requirements, assumptions, challenges.

1 Introduction

Today, ubiquitous access is not only a commodity for Internet users, but it is also essential to interact with the world. Moreover, mobile devices are increasingly widespread and are better equipped in terms of access technologies and service support. Moreover, mobility is an essential key feature which holds specific network requirements. For instance, any movement across different network segments should be transparent to the user, so that the network should be able to maintain service continuity independently of location and access media, supporting the heterogeneity of today’s networks and technologies.

Mobility management is today an intrinsic feature of mobile networks. However, it is still a feature left aside in what concerns the most recent trends in wireless networking, namely, in user-centric environments. In these environments, the social behavior inherent to humans is also impacting the way network access is perceived;

K. Pentikousis et al. (Eds.): MONAMI 2010, LNICST 68, pp. 340–353, 2011.

they consider that users develop spontaneous wireless networks simply based upon cooperation and access sharing on particular communities. Such user-centric architectures bring in several challenges to the traditional and tightly controlled mobility management schemes. First, in user-centric scenarios, the network elements are usually devices either carried or controlled by regular Internet users or providers. Second, users share subscribed Internet access. Third, users (and hence, the devices they own) tend to be mobile, with large dynamicity. Fourth, in these networks, some access control features may be transferred by the provider to the control of the user (as it is the case of femtocells).

Current mobility management solutions are not optimized for the previously described aspects, mainly personalization and dynamicity. It is therefore of major importance to re-think mobility management from an out-of-the-box perspective, and in particular, to consider user-centric approaches and how these can assist not only the individual user but also the provider in terms of mobility management coupled to the day-to-day living of Internet users. Such re-thinking has to consider trends on personalization and dynamicity: it is required to pro- vide a mobility process applied to distinct users with different mobility patterns, and also to different services and its characteristics, and forming different social networks.

As a first step towards a better re-thinking, this paper identifies and describes main user-centric scenarios, their assumptions, and mobility management requirements. We aim at assessing the suitability of current mobility models when applied to the described scenarios, and we show why a new approach and paradigm for mobility is required. For the sake of simplicity, one part of the discussion is divided in three blocks that we consider essential from a mobility management perspective: i) binding definition, what is the binding information and its initial discovery; ii) binding maintenance, how to maintain the translation/mapping update and at which cost; and iii) forwarding data problem, the required data plane techniques to keep up with the mutating control plane. We identify the main problems derived from the integration of these three steps in user-centric scenarios and propose some ideas to improve it. We analyze the cur rent problem of the use of IP address for both identification and location in the scope of mobility management and how it interferes with personal mobility, services mobility and multihoming. We further discuss initial ideas on requirements and characteristics of a mobility management architecture aiming at decentralizing the global management in user-centric scenarios, and exploiting how the context of users, networks and services can assist in optimizing mobility management. Finally, we analyze the distribution of mobility control points in the network according to different models and how they could be reallocated, based on adaptable principals that react to network changes.

This paper is organized as follows. Section 2 covers related work, also explaining our contribution in regards to previous work. Section 3 describes a set of user-centric scenarios, their mobility management assumptions and requirements, and their integration with current mobility solutions. Section 4 discusses challenges that we have identified and potential solutions to the identified gaps. The paper concludes with a summary and future work in section 5.

2 Related Work

To understand potential mobility patterns related to spontaneous environments, Huang et al. addressed the specific scenario of incident scenes, such as disaster networks and the need to provide connectivity on such environments [1]. The authors provided an analytical categorization of parameters that are related to mobility in such environments, and provide a set of recommendations to follow in regards to mobility in self-organizing networks. A study on an Urban landscape based on Google WiFi mesh network [2] provides a good basis for the analysis of wireless usage. In particular, the authors show that such usage is splitted into three classes mostly based on user devices, namely, traditional mobile computers (notebooks), APs, and PDA-like smart-phones. The authors also show that the urban mobility patterns exhibit the property of geographic locality. Specifically regarding accounting of mobile users in wireless environments, a solution considers the application of agents that track node mobility, the Mobile Agent (MA) middleware [3]. Such solution is based on having agents sent on demand to administer nodes. The central block works on the control plane only, in contrast to centralized mobility management solutions of today. A few proposals [4] [5] have considered the application of overlays to deal with mobility from a global perspective. This gives the means to consider mobility management from a distributed perspective, where the mobility anchor point may be placed within the user premises. However, these solutions do not consider de-centralization nor decoupling of mobility functionality. A proposal for a spontaneous environment mobility architecture based on the definition of more adequate addressing schemes, and hence, of more adequate routing [6], combines the notions of geographical routing based on ballistic trajectories with a location service based on Distributed Hash Tables (DHT) to achieve seamless mobility management in a k-neighborhood. Mobility management is based on the definition of an identifier that identifies the node on its constructed pseudo-geographical space and which associates the node with a k-neighborhood, thus providing an identifier to its mesh area.

3 User-Centric Scenarios

Broadband Internet access is in its majority complemented by wireless technologies in the last hop. Such wireless deployment, added to the low-cost and open-source firmware available, lead to a paradigm change in the user role in terms of networking architectures: the user today can contribute and assist in increasing the reach and support of the Internet broadband access. Hence, such networking scenarios correspond to user-centric scenarios in the sense that the user is capable of controlling its own wireless devices, which become part of the network.

The main aspects of user-centric scenarios relevant from a mobility management perspective are the following: high mobility frequency (users adhere to such wireless infrastructures mostly to be able to move freely across additional spots); nodes in the network that provide access to other nodes may change frequently; users share connectivity (share Internet subscription). To better analyse the implications of these aspects in terms of mobility management, we describe examples of scenarios with

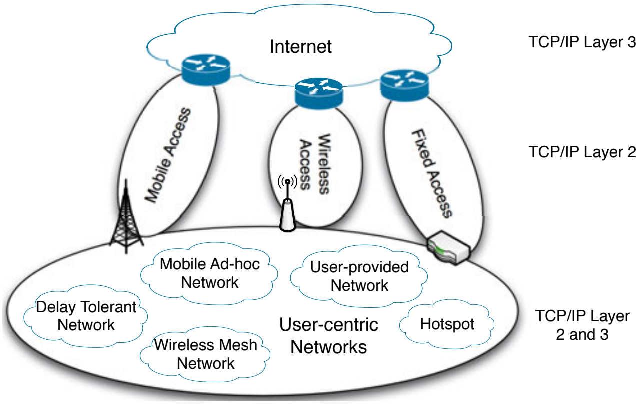

Fig. 1. Current Network Scheme

user-centric characteristics, as illustrated in Figure 1. We have considered five different architectures and we will analyze their main characteristics, common aspects and potential gaps to be filled from a mobility management perspective.

To support the comparison analysis, we provide Table 1. This table contains a set of main features that, jointly, characterize mobility management functionality: identification and user profile database, access control/authorization, service portability, resource management adaptation, and the potential need for local and global handover optimization.

Table 1. Systematization of the scenarios

Features/Scenario	Hotspot	WMN	MANET	UPN	DTN
Identification	Global user credentials, IP address	IP address (1 interface)	IP address (1 interface)	Community credentials, depends on local trust management system	Community credentials; may be provided spontaneously; local identification may not exist
User Database	Provider (access or service)	Community, provider	Provider (access or service)	Community, potentially distributed across several locations	Inexistent
Access control/ authorization	Centralized, provider	Distributed across a set of specific nodes	Distributed across a set of gateway nodes	Distributed and spontaneous	Decentralized
Mobility anchor point location	Edge node or Service Provider	Static gateway nodes	Static gateway nodes	Edge Node, Service Provider, Micro Provider	a few nodes on site, e.g. due to higher levels of residual energy
Portability	Local or dependent on 1 provider	Within a community (most likely tied to 1 provider)	Within a community (most likely tied to 1 provider)	Within a community (sometimes tied to a Virtual Operator)	Within a local area
Resource management adaptation	inexistent	inexistent	manual(nodes)	automatic	inexistent
Intra-handover frequency	low	medium	medium	high	high
Inter-handover frequency	low	low	medium	medium	low

3.1 Hotspot

The Hotspot is today the most popular architecture available with user-centric capabilities. Its main purpose is to expand and to complement current Internet broadband access. Wireless hotspots abound around us in residential households and public establishments (e.g. universities, shopping centers, hospitals, hotels). A Hotspot is composed by at least one wireless Access Point (AP) connected to the Internet through an Access Router (AR), being these devices usually provided by a Network Access Provider or an Internet Service Provider. Usually, the AR and AP are co-located (e.g. as part of the Residential Gateway on a household). In public Hotspots several APs may be connected to the same AR to provide a wider coverage area. Although in the hotspot scenario there is no connectivity relaying from one user to the other, the AP media is shared.

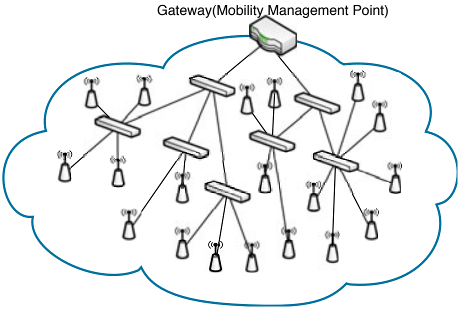

Fig. 2. Hotspot Scenario

The hotspot is controlled and owned by a provider. This is the case for our residential household, where we have an AP placed and controlled by our provider. Given that its purpose is to expand capillarity, hotspot users normally stick around and hence are said to visit a few preferred locations mobility is limited in scope (cf. first column of Table 1). Node movement speed is low (e.g. users walking on a house or to a coffee-shop), and connectivity while users move is intermittent.

Within a specific hotspot, movement is usually taken care of by the MAC layer. Moreover, user identification and authentication is provided by regular means based on MAC and IP identification, and controlled by the provider the user or a hotspot (for the case of pre-paid access) subscribes to. Hence, a hotspot is centralized, from an access control perspective. Service portability is an aspect that is only considered for hotspots belonging to the same provider, and resource management is usually inexistent, being the service provided on a best-effort basis. Consequently, the need to perform handovers normally relates to inter-hotspot scenarios, where users arrive or leave a hotspot. When inter-hotspot handovers occur, they are dealt with from an OSI Layer 3 perspective.

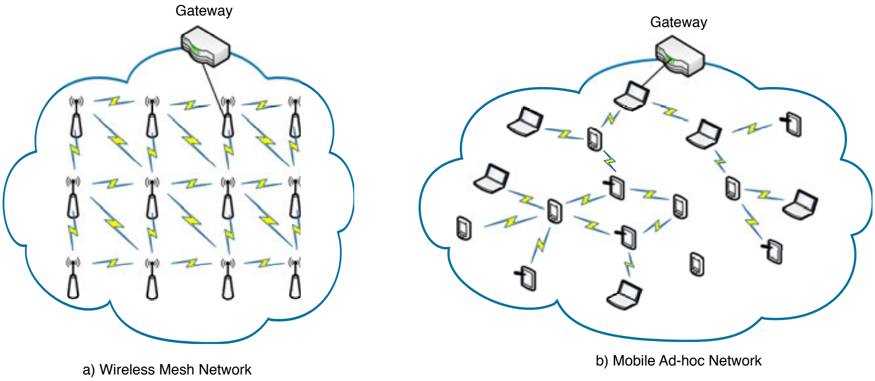

Fig. 3. MANET and WMN Scenarios

3.2 WMN and MANET Scenarios

Wireless Mesh Networks (WMN) and Mobile Ad-hoc Network (MANET) scenarios, which are respectively covered by the second and third columns of Table 1, are both sub-cases of ad-hoc networks. A main difference to highlight between WMNs and MANETs is that, while in WMNs all nodes are static, in MANETs all nodes may move, even though today most of the gateways are static. Both these scenarios have intrinsic characteristics that must be considered when addressing mobility management.

Similarly to the hotspot scenario, these scenarios are also applied to provide connectivity expansion in an autonomous way. However, it should be noticed that for this specific case (and in contrast to the hotspot model), the provider has no control on the MANET growth/operation. Hence, key aspects to take into consideration in this model are the clear split of network management functionality between the access and the MANET (Customer Premises) region. Moreover, there is no centralized control and hence, ad-hoc transmission brings both benefits and disadvantages (e.g. overhearing). Central to the deployment of this scenario is the need to consider a dynamic routing (multi-hop) protocol, to ensure reliable transmission across several hops.

The gateway nodes are, from a mobility management perspective, crucial nodes in the sense that the mobility anchor point may be co-located with theses nodes. Moreover, gateway nodes are also relevant in terms of access control.

Portability is also a feature that is limited to the scope of a specific community or tied to a provider.

3.3 User-Provided Networks

User Provided Networks (UPN) aspects are presented in column four of Table 1. UPNs relate to a recent trend in spontaneous wireless deployments where individual users or communities share subscribed access in exchange of incentives. Hence, the user becomes a provider of services given that by sharing Internet access users devices become networking devices, for instance, they relay connectivity. This

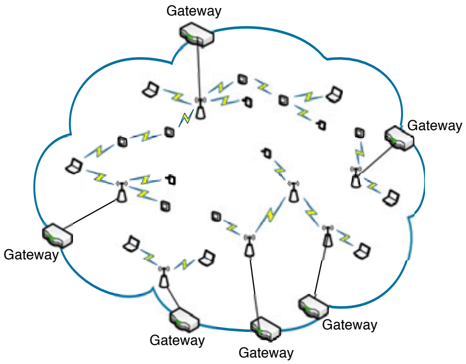

Fig. 4. UPN Scenario

aspect is not completely synchronized with the Internet end-to-end principle, which describes a clear functional splitting between end-systems and the network. A key aspect to UPNs is that they rely on existing network topologies, as illustrated in Fig. 4.

We can divide the UPNs according to two main types: infrastructure-based and mesh-based. Both types are being applied as complement to existing access networks: they allow expansion of such infrastructures across one wireless hop. For both models, there is usually one individual or entity (the Micro-Provider, MP) which is responsible for sharing its connection with N-1 other users (out of a universe of N users, who today belong to a single community). Moreover, a user is, in a specific community, simply identified by a virtual identifier (a set of credentials username and password) which is stored by a Virtual Operator (VO) and rely upon whenever the user decides to access the Internet by means of a specific community hotspot.

To better illustrate examples of UPNs, we here consider three different scenarios. In the first scenario, a hotspot owner willingly shares the Internet access with specific friends, using a local authentication procedure. The requirements and assumptions of this scenario are similar to the ones of the Hotspot model.

Another scenario corresponds to the regular municipality Wireless Fidelity (WiFi) case, being the user authentication local. In this scenario, the network adopts a mesh topology, so the characteristics and requirements of this scenario are similar to WMN, previously analyzed. The last UPN corresponds to a residential scenario, where a regular user at home decides to open access to a specific community, which is managed by a VO (cf. Table 1). The only relation the MP has to the VO is that the MP belongs to the community coordinated by the VO.

In terms of mobility management, UPNs are expected to exhibit more variability than the previously described scenarios given that user equipment is part of the network. For instance, a user can turn off his equipment at any time without previously notifying users profiting from the relayed connectivity. The impact of having users controlling portions of the network is highly related to the underlying network architecture(s): such impact may be local or propagated to the whole network. From a mobility management perspective, the MP is the crucial point to consider. The VO (in contrast to scenarios where the provider performs mobility management) is simply a coordinator for access control.

In terms of handovers, the UPNs privilege the inter-UPN handovers among MPs of users of the same community. The idea of the UPN is to provide connectivity in a large area to a user that belongs to the community. The user can move inside of a certain area, maintaining the connectivity from several access points. In general, the size of each UPN is small, so the requirement of intra-UPN handovers is not high.

3.4 DTNs

Delay Tolerant Networks (DTN) are used for chaotic conditions, like natural disasters, wars, accidents or space networks. These networks have completely different paradigms comparing with the previous ones. DTN is a concept an not a network topology or technology, since it can be applied to current network structures in disruptive and chaotic scenarios, as presented in Fig. 5. DTNs present intermittent connectivity, long and variable delay, asymmetric data rates and high error rates. The main purpose of DTNs is to deliver vital messages without losing any information, independently of the delay and connectivity. In these scenarios, some messages are stored in some nodes along the path until being possible to forward them. The traditional end-to-end notion of the transport protocols, like Transport Control Protocol, is impossible to be applied to DTNs.

In DTNs, the access control and authorization is decentralized through the network elements that form the DTN. The dimensions of the DTN depends on each scenario, from small spaces with disruption of connectivity, such as rural places, to the large and sparse places when natural disasters occur. DTNs could exist across different access technologies, and it is important to exploit all connectivity points and resources available, since they are reduced and sparse.

In DTNs, the identification of the user is provided spontaneously by the community, since the user database is inexistent. In this scenario, the identification of each user, regarding his community role and qualification, is extremely important. Besides the importance of the identification, its relevance depends on the location tracking process that is vital for the mobility management.

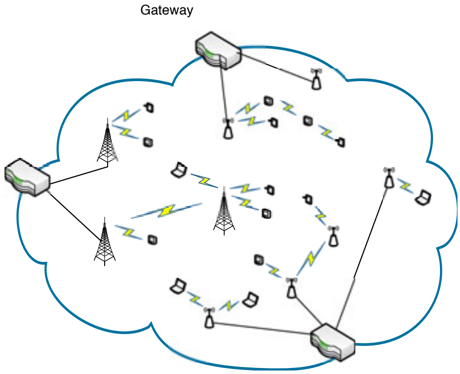

Fig. 5. DTN Scenario

In DTNs, users usually transport information, while they move along the entire network. When a user finds a connectivity point in the network, he delivers all stored information to the next storage point (other user or network element). The handovers between the DTN and the outside are not common and rarely happen, so the mobility management should consider the intra-DTN as the main priority.

3.5 Mobility Issues

In this section, we discuss the efficiency and applicability of the current mobility assumptions, requirements and solutions in user-centric scenarios. We discuss the main requirements and assumptions to improve the mobility management in the chosen scenarios, analyze the main advantages and drawbacks of the existing mobility solutions for each scenario, and identify the aspects that can be changed to improve each scenario.

Hotspot is implemented under a tree topology network model; therefore, gateways are strategical and natural points where communication messages travel, especially in inter-hotspot communications. The implementation of a mobility control point in the gateway is obviously an efficient solution, since the distance in hops between the gateway and a generic mobile node is, in average, the smallest in the entire hotspot. Moreover, data traffic between the hotspot and the outside is forced to cross the gateway, so it can be easily forwarded. In general, gateways are present in almost every user-centric scenario, being good elements for mobility control and even traffic forwarding. It is important to remember that most of the current hotspots already use bindings through Network Address Translation (NAT) to map the private IP/port addresses into a global IP/port address. The current mobility solutions can deal with the hotspot scenario, but not in a efficient way. The fact that it is required to send traffic to the home agent ([7]) every time a user wants to communicate with another one is one of the problems. Moreover, when the MN changes from one hotspot to another near the previous one, the user needs to inform its correspondent node of its new location, so that the correspondent node sends the packets directly to the new location. Another issue with current Mobile IP (MIP)-based solutions ([7], [8], [9], [10]) is that the home agent is associated with the gateways, so if the gateway fails, the home agent gets unavailable and the nodes belonging to that home agent will not be located by other nodes. In specific situations, where the hotspot has large dimensions and the user moves inside a small part of the hotspot, a control point in a network element that covers only the area visited by the user can be introduced, optimizing the mobility process, but also introducing a new level of control.

WMNs and MANETs implement mesh topologies, so they are substantially different from the Hotspot model. Although the traffic between the ad-hoc network and the outside needs to cross the gateway, interior traffic does not. Thus, gateways usually are implemented in the border of the ad-hoc network. In this sense, it is possible that a mesh node with fewer hops to a certain mobile node than the distance to the gateway, can take part on the local mobility management, specially in large WMNs. This solution is possible only for WMNs, since the mesh routers are stable and fixed. Specially in large WMNs, a control unit inside the network can decrease the overhead of control and improve the time to react to changes. Data packets are routed through wireless hops, delaying the delivery, which depends on the load to access the medium, in a considerable time. The current MIP-based solutions only implement the mobility control up to the gateway, so these assumptions require significant changes. In a MANET, it is difficult and dangerous to select a control point in the middle of the network, since the routers, composed by the mobile nodes, are constantly moving and changing routes and topology. Therefore, it is better to implement the control functions only up to the gateway or in specific situations where the user has appropriate patterns that relate to stability. The current mobility management solutions do not cope with the dynamics and adaptability of the mobility control points along time. It is important that a user is able to subscribe a new mobility control point, not only when the previous one goes down, but also when a new one offers better conditions.

The UPNs bring different paradigms in mobility management, since a mobile node can use a wireless access network according to the user that becomes a Micro-Provider (MP); therefore, a MP can switch off its network equipment and the users in this UPN will lose the internet connectivity. In this sense, the users that become MP need to have specific stability patterns. We can have several MPs near each other, sharing their internet connection with other members of the same community, so, it is useful to exploit mobility control mechanisms among them for users that spend their time using these MPs to obtain connectivity. In some scenarios, these MPs can create a mesh network with their devices, being connected by two different ways. These cases, together with specific patterns of the users, provide the substrate to introduce mobility control inside the UPNs. The current solutions of mobility are not prepared to cope with these dynamic scenarios, where gateways and other network elements are constantly changing. Thus, home agents and mobility anchor points should not be statically defined in a certain network element; they should have the capability to be transferred to other points, reacting to the network behavior. In these scenarios completely focused on the user as the last access, the identification of each user should be taken into account, since most of the current mobility solutions do not use it, defining the IP for both location and identification.

DTNs present different characteristics and assumptions when compared to the previous ones. These networks can have both structured and unstructured parts forming the entire network. This scenario then covers several concepts of the previous scenarios, where spontaneity, dynamics, social and priority are the main paradigms. These networks are not controlled, but it is important to assure that different entities have different priorities to properly operate, such as in a natural disaster. The messages must be delivered without losing packets in the communication. The location part of mobility management is of great importance for this kind of applications, since we need to find as fast as possible the designated user and send him the vital information. In this scenario, the mobility control points should be very dynamic, since the network changes all the times, according to network, users and environment. In this case, it becomes important to introduce the control points near the most important users and in strategical places according the environment, inside the DTN. The search for control points needs to be very fast, since some devices carry with them vital information that should be forwarded to the network as soon as possible. Currently, no mobility solution can handle with chaotic scenarios, since it was not envisioned for these applications. The mobility management solution for this scenario should be analyzed from a different perspective, integrating adaptability, spontaneity and personalization (e.g. identification and qualifications) in a overall mobility management solution.

4 Challenges of Mobility Management

In this section, we discuss the main issues in mobility management when dealing with user-centric scenarios, which will then be used to derive the fundamentals of a user-centric mobility management architecture. Fig. 6 illustrates the main challenges and initial ideas to improve the mobility management.

The current Internet model uses the IP address for both identification and location. In the Future Internet, it is expected that the IP address will only represent the location of a certain device according to the distribution of the IP addresses. The identification may not be connected to the IP address, since the user may change access network, use multiple interfaces and several devices. In this sense, binding definition needs to be re-thought to integrate the user's identification in the binding mechanism: this would allow the update of all IP addresses of the different interfaces, independent of the location and device of the user. Moreover, it provides the base to develop personal mobility, exploit multihoming, and increase the flexibility in the mobility management supported, enabling the user to be connected to different networks and mobility control points according to the services, network conditions and user requirements.

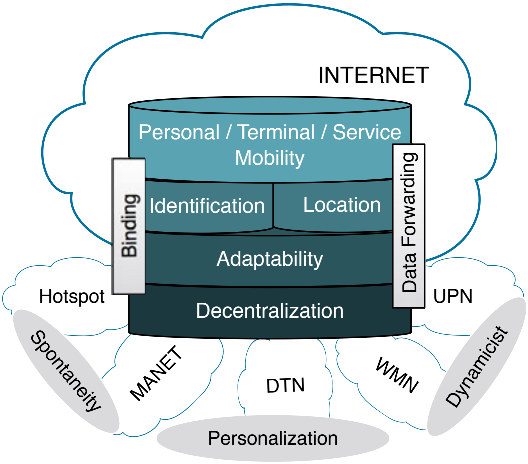

Fig. 6. Challenges for Mobility Management

Current mobility solutions define mobility control points, like the Mobility Anchor Point (MAP), in order to maintain the bindings of the mobile nodes. The control plane is separated from the data plane, since the binding update process is independent of data forwarding. However, it is not clear if control plane shall be completely separated from the data plane. Considering that the routing and similar mechanisms are part of the control plane, current mobility solutions are more concerned with the control plane, specially the bindings maintenance; data forwarding is treated with the same approaches in the different scenarios. One possible solution for this problem is the development of two separate structures, one dealing with binding and another dealing with the data forwarding. These two structures need to be integrated in order to provide the best results for the general mobility management approach. This idea provides flexibility in the selection of both structures, since control binding elements require less resource than the data forwarding elements. Another possible solution is to develop an approach that deals with both parts, defining elements that, not only maintain bindings, but also decide on the traffic forwarding. This approach does not need the communication of the two structures, reducing overhead and time to react to events. However, it is much more rigid in the selection of the elements, since they will receive and send traffic not destined to them.

User-centric scenarios, as explained before, present several requirements, which dynamicity, spontaneity and personalization are some of them. In order to provide mobility management in these scenarios and according to the previous discussion on control and data traffic, the control points (bindings and data) must adapt to network changes, as illustrated in Fig. 7. These control points should be dynamically selected according to current network information, users information and services. When a control element fails (it moves or shuts down), the control mechanism needs to be moved to another element of the network. Besides failures, the control point could be moved to optimize resources and improve the general performance of the network (Fig. 7). A network element shall be able to recognize its neighbors that are available to be control points. Each control element should be classified according to context information in order to produce a ranked list of the neighbors' control elements (several ranked lists may exist according to user and services context). If a control element is shutting down, it selects the best one of the neighbors' ranked list and interacts with the selected control element to transfer the stored information and functions. As discussed in subsection 3.6, the distribution of mobility control points depends on the user-centric scenario. If binding and data control are aggregated in an unique structure, mobility control points will be advantageous when implemented in the gateway or edge node. However, if control points for binding and data are separated, the control binding points can be implemented inside the user-centric network, specially in the WMNs and DTNs.

Finally, we discuss the method to place the control points through the network. The four main approaches are: centralized, hierarchical, decentralized and distributed, sorted from the most central to the most distributed. Each one has advantages and disadvantages, regarding binding maintenance and traffic forwarding. In the centralized approach, it is easier to update and search for bindings, since the central point is well-known, never changing. However, the centralization of the binding storage increases overhead and latency when a user wants to communicate with a near one, since each user needs to constantly update his location to the central point. Centralization has another disadvantage regarding tolerance to failures, since it is a unique point of failure. Regarding the data forwarding, it has several disadvantages,

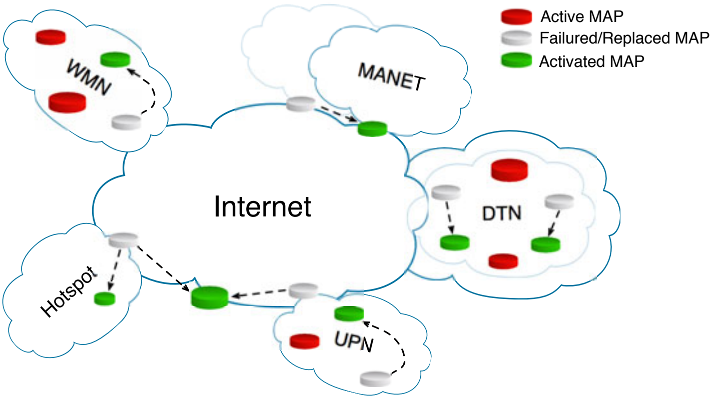

Fig. 7. Principals for Mobility Management

where one of them is the unique point of failure. Forwarding traffic with a central point implies that all traffic crosses this point, increasing the packets load near the central point and causing an unload-balanced traffic in the network. Another problem is the time to redirect traffic to the new location of the user, since the central point is far away from user. The hierarchical approach presents the same problem of failure, since we have several levels and the higher level usually is a central point that controls several lower levels. However, this solution introduces scalability, since it allows a more efficient binding search and update when a user wants to communicate with a neighbor, since it only uses lower levels for updating and searching. The data forwarding in hierarchical approach presents similar problems to the centralized approach, since it needs to cross the central point of the higher layer of the hierarchy. The decentralized approach is the most balanced, since it distributes the bindings across several points, according to a predefined criteria. So, it is much more tolerant to failure than centralized or hierarchical. Depending on the size of network, this solution can use different number of control points; they are relatively near to users, being easier and faster to update and search for users. However, decentralization implies an efficient method to distributively search for user location, or to synchronize the decentralized nodes. Regarding data forwarding, decentralization allows to redirect data to the current user's location in a fast way, without a significant impact in the overhead and load balancing. The last method is the distributed, where all nodes of a network participate in the mobility management. This method is the most tolerant do failures, since, even with several failures the network continues to work. However, this approach requires a large overhead and intelligence to search for a user's location. The simplicity in updating process increases the complexity in the searching process. Another problem is the update of information among the entire nodes, that increases not only the overhead but also the time of synchro- nization. This time needs to low, since several events (search and update) are constantly happening and the answer to these requests should be according to the latest network information.

5 Conclusions

This paper assessed the efficiency and applicability of current mobility assumptions in user-centric scenarios, addressing their requirements and solutions when applied to several types of networks that may exhibit user-centric characteristics, such as hotspots, wireless mesh and ad-hoc networks, user provided networks and delay tolerant networks. This study showed that current solutions of mobility are not prepared to cope with most of the scenarios: they may not be efficient (hotspot), they do not cope with the dynamics and adaptability of the mobility control points along time (WMNs, MANETs and UPNs), or they are not prepared to specific scenarios (DTNs). This paper also identified the fundamentals of a user-centric mobility management architecture able to efficiently deal with the aforementioned scenarios, such as: the integration of the user's identification in the binding mechanism; the coupling and decoupling of both control and data planes; the support of dynamic control points according to network conditions, user and service requirements; and the decision on where to place the control points in the network. The definition and specification of the user-centric mobility architecture, addressing the several issues discussed here, will be left as future work.

References

1. Latré, S., Simoens, P., De Vleeschauwer, B., Van de Meerssche, W., De Turck, F., Dhoedt, B., Demeester, P., Van den Berghe, S., de Lumley, E.G.: An Autonomic Architecture for Optimizing QoE in Multimedia Access Networks. Comput. Netw. 53(10), 1587–1602 (2009)
2. Akyildiz, I.F., Xie, J., Mohanty, S.: A Survey of Mobility Management in Next-generation All-IP-based Wireless Systems. Wireless Communications 11(4), 16–28 (2004)
3. Hussain, S., Hamid, Z., Khattak, N.S.: Mobility Management Challenges and Issues in 4G Heterogeneous Networks. In: InterSense 2006: Proceedings of the First International Conference on Integrated Internet Ad Hoc and Sensor Networks, p. 14. ACM, New York (2006)
4. Kumar, B.P.V., Venkataram, P.: Prediction-based Location Management Using Multilayer Neural Networks. Journal of Indian Institute of Science 82(1), 7–21 (2002)
5. Samaan, N., Karmouch, A.: A Mobility Prediction Architecture Based on Con- textual Knowledge and Spatial Conceptual Maps. IEEE Transactions on Mobile Computing 4(6), 537–551 (2005)
6. Lei, Y.-X., Kuo, G.-S.: Impact of MAP Selection on Handover Performance for Multimedia Services in Multi-Level HMIPv6 Networks. In: IEEE WCNC 2007 Wireless Communications and Networking Conference, pp. 3901–3906 (11-15, 2007)
7. Johnson, D., Perkins, C., Arkko, J.: Mobility Support in IPv6 (MIPv6). RFC3775 (Proposed Standard) (June 2004)
8. Soliman, H., Castelluccia, C., Malki, K.E., Bellier, L.: Hierarchical Mobile IPv6Mobility Management (HMIPv6). RFC 4140 (Proposed Standard) (August 2005)
9. Koodli, R.: Fast Handovers for Mobile IPv6. RFC 4068 (Proposed Standard) (July 2005)
10. Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., Patil, B.: ProxyMobile IPv6. RFC 5213 (Proposed Standard) (August 2009)