A COHESIVE TECHNO-BUSINESS VISION FOR FUTURE WIRELESS NETWORKING

Ivan Ganchev

Abstract: *This paper proposes a cohesive vision for future wireless networking, based on a novel generic techno-business model, which – while different from the evolving legacy one – is both feasible and attractive to stakeholders, and could drive the '5G and beyond' vision for future generations of wireless communications. The technical implications of the proposed model are explained and the key technological innovations required to support it are outlined.*

Keywords: *Consumer-Based techno-business Model (CBM), Always Best Connected and best Served (ABC&S), Ubiquitous Consumer Wireless World (UCWW), Third-Party Authentication, Authorization and Accounting (3P-AAA), Consumer Identity Module (CIM) card, Personal IPv6 (PIPv6) address.*

ACM Classification Keywords: *C.2.1 Network Architecture and Design – Wireless communication, C.2.2 Network Protocols – Protocol architecture, D.2.2 Design Tools and Techniques – Evolutionary prototyping, D.4.6 Security and Protection – Authentication.*

1. Introduction

This paper puts forward views on evolving fifth generation wireless world and how that evolution may be directed for the benefit of the consumers and other stakeholders. It argues that an infrastructural re-think on the way Authentication, Authorization and Accounting (AAA) service is supplied is the key to this evolution. At a high level this may be described as a business plan for the supply of mobile services, especially with the wireless access service component being founded on a consumer-based structure rather than on a subscriber-based one. The novel Consumer-Based techno-business model (CBM) will enable a loose dynamic (even casual) consumer-type association between mobile users (MUs) and access network providers (ANPs). Innovations required to support this include a pivotal role of a third-party AAA (3P-AAA) service provider entity.

The view on the next (5G) generation of wireless communications, employed in this paper, is the one which encompasses all existing, planned and future mobile and fixed wireless networks, both terrestrial and satellite. The goal is to sell services to a great market of users in overlapping local, regional, and global domains; to create a Ubiquitous Consumer Wireless World (UCWW), where connectivity will be available anywhere-anytime-anyhow and services will be rapidly deployed on-demand, customized to the user's needs, and adapted to the current user context and network context, in the best possible way independent of the user's movement across heterogeneous access networks. This vision requires unprecedented levels of autonomy, application service adaptability, and network element integration at all levels including mobile devices, access networks (ANs), and core networks. Other terms that characterize this 5G vision include dynamic quality of service (QoS) provisioning, and network- and device dynamic reconfigurability. From access networks point of view, especially that based on the existing Subscriber-Based techno-business Model (SBM), the challenges this 5G vision raises are convergence, integration, and interworking of existing and emerging heterogeneous wireless networks, in order to provide users with all their desired services in a seamless Always Best Connected and best Served (ABC&S) way.

For the mobile user, the experience of ABC&S communications services should preferable move towards having consumerist-type characteristics where, through user-friendly interfaces, ABC&S decisions are user-driven and user-executed. ABC&S scenarios should enable mobile users to move seamlessly between different wireless access networks according to their own criteria (e.g. on the basis of price/performance ratios), while maintaining active service sessions, i.e. without interrupting service sessions, restarting applications, or losing data. The CBM model, promoted and further explained in this paper, would foster this new type of wireless network environment, called the UCWW. It is much less constrained than the SBM model widely used today, which in fact would militate against many aspects of it. Section 2 provides more details on the novel CBM model in comparison to the existing SBM model.

A real drive towards an open ABC&S UCWW paradigm has the potential to gradually restructure the existing subscriber-based business realization of mobile communications, transforming it into a consumer-based one. In this it raises important challenges for existing ANPs (i.e. mobile operators) and opens new opportunities for new ANPs, aiming to fill niche markets. For a new ANP entrant, it would mean the possibility of ease of entry and of having dynamic (even casual) consumerist-like relationships with users, i.e. offering and providing services to them without any prior business relationship and subscription. Significant re-thinking and breakthroughs in the way traditional AAA services are provided are necessary. One of the main challenges is the creation of a framework for strategic infrastructure and protocol development for independent autonomous provision of AAA services by third parties (3P-AAA), which are not network providers. This concept, the foundation stone for a re-structured business plan for the provision of wireless services, is presented in Section 3.

The CBM model utilizes a novel concept of a personal IPv6 (PIPv6) address, which enables advanced mobility, i.e. in ways not presently possible, and continued participation in various evolving communications scenarios. Through an enhanced AAA functionality, the PIPv6-based CBM model also has the potential to enable commercially viable ad-hoc and/or open mesh-networking solutions, where a mobile node (object) acting as a gateway (or relay) may offer (or facilitate) wireless Internet access services casually or persistently to other mobile nodes/objects and be paid for this service, e.g. through a 3P-AAA service provision. Realization of this would bring about a radical change to the access network business, and add many new ways whereby mobile users will be able to gain access to network services. More details on the PIPv6 address mechanism along with a corresponding generic communication scenario are presented in Section 4.

A typical implementation approach for the identification and authentication of mobile users (MUs) on mobile devices today is by means of a subscriber identity module (SIM) card inserted in the corresponding device currently used. In the UCWW, this type of card will be replaced by a new type – a smart consumer identity module (CIM) card – which will contain the user’s credit card details, or a specific authentication code acceptable/provided by a 3P-AAA service provider (3P-AAA-SP). This way each service charge, incurred by the user, will be paid indirectly through the 3P-AAA-SP, who will then arrange relevant payment to the corresponding service provider. Section 5 deals with the CIM card aspects.

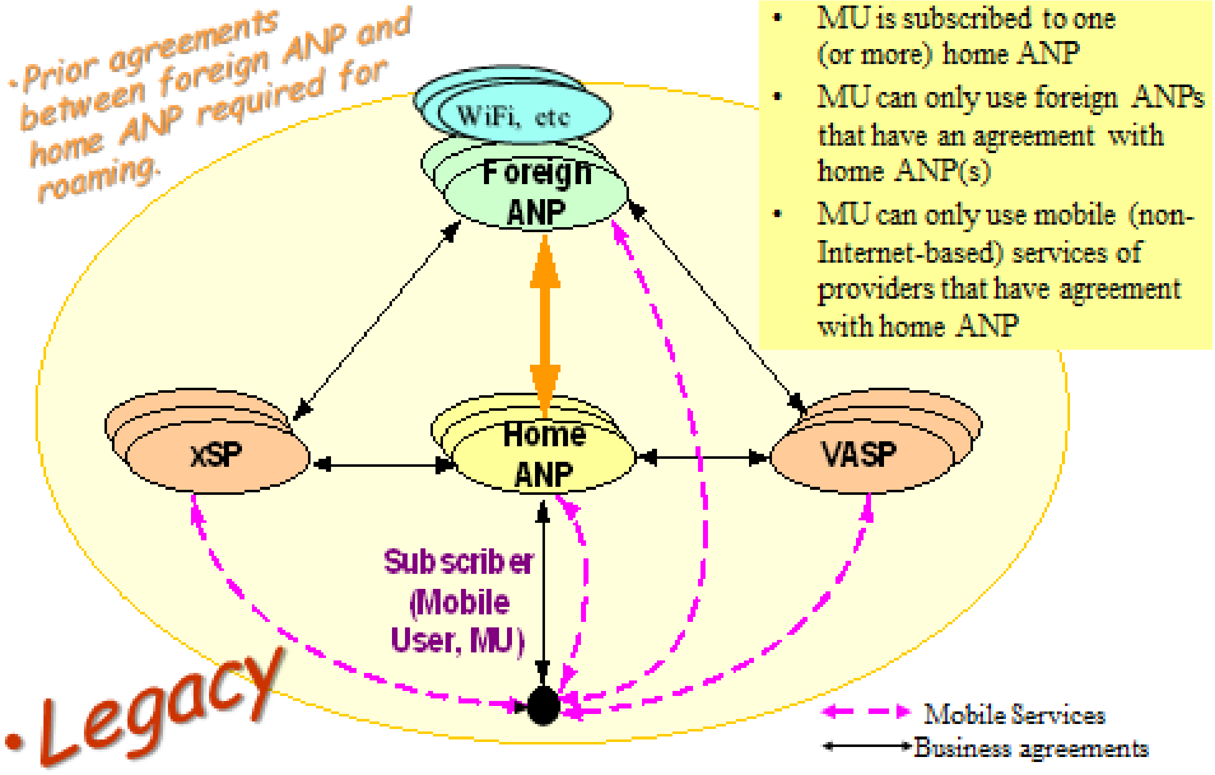
2. Techno-Business Models

Important in the process of bringing about this ABC&S UCWW reality are the questions of feasible techno-business models:

- What kind of generic model(s) would be attractive to stakeholders and would drive this 5G vision?
- What are the technical implications of such models?

The existing and widely used SBM model is founded on the necessity of a mobile user (MU) having a contract (an account) with at least one ANP before s/he may start using mobile services. For the MU, this ANP is called the home ANP. The user is a **subscriber** and as such has a mobile number(s) tied to that home ANP. Even though the mobile phones may have multiple SIM cards inserted, equivalent to having a number of subscriber contracts with different ANPs, this is not user friendly and the mobile numbers are under the control of home ANPs, even where number portability is facilitated. Relative to the home ANP, all other ANPs are termed foreign or visited ANPs. Prior roaming agreements between foreign and home ANPs are required in order for MUs to camp on them. Similarly, the mobile service providers (xSPs) are able to offer their services (excluding those, of course, that could be accessed/obtained directly on/from the Internet) through ANP networks under respective prior business agreements with them directly or indirectly through value-added service providers (VASPs[*]). The key idea of the SBM model is that the user is being locked-in as a subscriber to a particular ANP for a long time. The general trend today is to continue with this model, which mostly benefits the existing ANPs (i.e. the dominant cellular mobile operators) and converts into a pipe-dream the entire idea of using the access network simply as a section of service-independent transport pipes [O'Droma, 2004b].

In this ANP-centric SBM model, the home ANP is placed at the center as both the effective manager of the user's wireless communications and AAA activities, and the supplier of part of the wireless communication services (Figure 1). It may be well argued that this uniquely strong position of the home ANPs, with its potential to constrain the users' freedom and independence, by the fact of their being 'subscribers' more than 'consumers', in seeking better value for money, is inimical to the user's best interests [O'Droma, 2004a].


• Prior agreements between foreign ANP and home ANP required for roaming.
WiFi, etc
Foreign ANP
xSP
Home ANP
VASP
Subscriber (Mobile User, MU)
• Legacy
Mobile Services
Business agreements

- MU is subscribed to one (or more) home ANP
- MU can only use foreign ANPs that have an agreement with home ANP(s)
- MU can only use mobile (non-Internet-based) services of providers that have agreement with home ANP

Fig. 1. The SBM with the home ANP at the center

[*] VASPs provide additional services related to, e.g. ordinary service deployment and adaptation to user/device/network profiles, special service configurations, transparent network and mobile device reconfigurations, service adaptations to satisfy special service requests, etc.

It will always be difficult to escape the constraints and limitations effected by the home ANPs for their own business reasons including those serving dominance goals within the AN market, and even within the market of the mobile service providers (xSPs). It will also be a difficult business place for new ANP entrants as the business agreements with other ANPs for interoperability, interworking, AAA etc., and with many crucial xSPs, will always be a critical and necessary component for their entry and survival, as well as having to have in place customer administrative and management support before they might hope to start seeking ‘user (subscriber) accounts’ and make inroads into the market, and face the task of convincing great numbers of potential users, who are probably already subscribers to competing long standing ANPs, to become their subscribers. This is the inherent nature of the SBM model [O’Droma, 2004a].

Naturally the problems with the SBM will put a brake on fast deployment and flexible provision of new services and ANs, as well as result in significant insecurity for (barrier to) new xSP entrants because they will need prior xSP-ANP business agreements, which is slow and time-consuming process. In addition, it will cause slow, constrained ABC&S 5G evolution due to the fact that the mobile user must be a subscriber to an ANP before may access their ABC&S offerings, and will find him/herself constrained to these. While in the short term this path of 5G evolution may benefit existing cellular wireless license holders, in the long term it will be to the detriment of all, with the likely appearance of disruptive wireless technologies leading to the specter of serious fragmentation in the absence of the core elements of a technological foundation for a structured business plan, through which such technologies can be brought into easy access for customers. Thus the SBM is considered as a legacy techno-business model [O’Droma, 2004a].

Within the context of the shortcomings of the SBM, the alternative CBM model comes with many attractions for the evolving ABC&S UCWW. In this model, the mobile users (MUs) do not have formal subscriber relationships with ANPs and thus may act as **consumers**, not as subscribers. This is much like other consumer services, e.g. the shopping of goods on a street or in the mall. Moreover in the CBM, the MU owns his/her mobile numbers (e.g. IPv6 addresses) as of right and this is not subject to any ‘subscriber agreement’ as the consumer-user does not have a subscriber contract with any ANP. This allows him/her to request different types of services from different types of (mobile) service providers (xSP), which services are provided through multiple service-specific ABC&S wireless access connections which best match the consumer’s profile/role. In the CBM, there is no distinguishing between home ANPs and foreign/visited ANPs; they are simply called ‘ANPs’. They provide access network infrastructure and transport medium. Examples include cellular (2G/3G/4G) mobile operators, Wireless Local Area Network (WLAN) providers (utilizing the IEEE 802.11 standard) with corresponding Wi-Fi hotspots, WiMax providers (based on the IEEE 802.16 standard), etc.

A key CBM element is that it separates out the administration and management of users' one-stop-shop authentication and accounting system from the business of supplying a wireless access network service, and locates it with a third-party AAA service provider (3P-AAA-SP), who is not traditionally a stakeholder in the wireless communications business. Through business agreements with such 3P-AAA-SPs, all types of providers (ANPs and xSPs) will be able to offer their charge- or fee-based services to MUs who have credit arrangements with one or more 3P-AAA-SP, just as they have one or more credit cards today, and similarly through this entity will receive periodic itemized bills for all services where they incur costs, which have been paid through this 3P-AAA-SP. This way all ANPs and xSPs charges will be paid indirectly through 3P-AAA-SPs. In the case of a MU using multiple 3P-AAA-SPs, the MU's choice of 3P-AAA-SP at any time for any service will be dictated by decision processes similar to those occurring today when deciding which credit card to use for a particular bill. However, this will be done mostly transparently to the user, based on his/her predefined preferences [O'Droma, 2004a]. In this case, the 3P-AAA-SP becomes the central player. An explanatory example of this consumer-based business plan structure is illustrated in Figure 2.

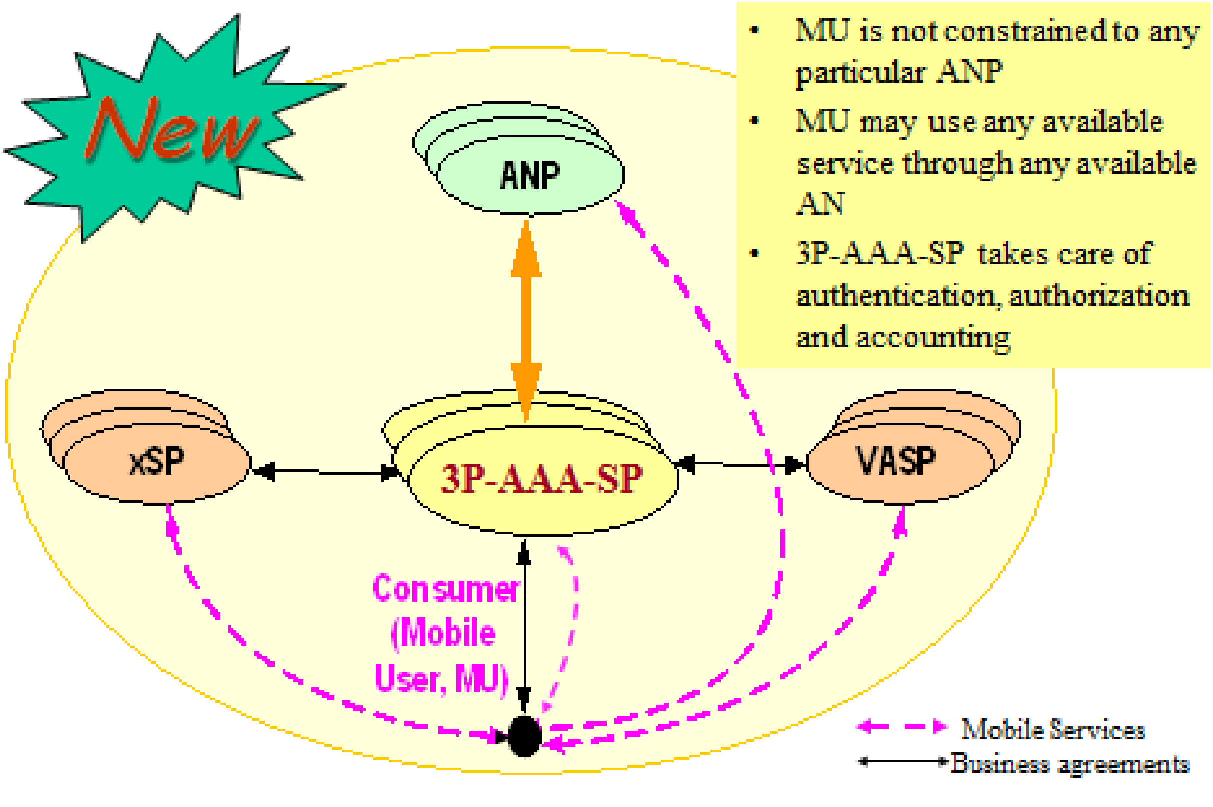

New
- MU is not constrained to any particular ANP
- MU may use any available service through any available AN
- 3P-AAA-SP takes care of authentication, authorization and accounting
ANP
xSP
3P-AAA-SP
VASP
Consumer (Mobile User, MU)
Mobile Services
Business agreements

Fig. 2. The CBM with a third-party AAA service provider (3P-AAA-SP) at the center

In the UCWW, established on this CBM model, the MU will be identified by a smart consumer identity module (CIM) card, replacing the legacy SIM card. The CIM will contain the user's credit card details and/or a specific authentication code acceptable, or even provided by, the 3P-AAA SP. This way each service charge (e.g. to ANP or xSP) may be paid indirectly through a 3P-AAA-SP, indicated by the payee. Financial institutions, such as present-day credit-card companies, would probably be the most suitable contenders for the 3P-AAA-SP business [O'Droma, 2004a].

Besides giving the MU much greater freedom of movement, through the creation of a more open access-network and mobile-service market with easier and fairer access, this network-independent business model foundation and facility would be particularly attractive to new ANP entrants, and to existing ANPs and xSPs trying to extend their market share, streamline their business, fill niche and specialized AN service provision, and so forth. It has the potential to open the wireless communications market thus facilitating the new entrants. It will provide wider range of freedom and autonomy for ANPs (especially new ones), levelling the AN playing pitch and fostering real ANP competition. For MUs, it will provide a lot of more benefits in terms of greater range of ABC&S offerings as an important business driver for the evolution of ABC&S 5G networking. Other pros include fast deployment and flexible provision of new services, preventing scalability problems, no real differentiation between home ANPs and foreign ANPs, leading to reduction and even elimination of roaming charges, which is completely in line with the EU directives (i.e. a local call will always be a local call regardless of where the user has roamed to!) [O'Droma, 2004b].

The CBM has inherent business attributes to drive forward the evolution of ABC&S networking, as both competition, interoperation, and collaboration advantages will be underpinned by efforts to provide a wide range of QoS offerings with greater flexibility and with a wider range of price/performance ratio options in the efforts of providers to attract in greater numbers of service users. With this novel approach a real accomplishment and true meaning of the word 'mobile' will be reached in relation to 'mobile devices' as these will no more be tied (locked-in) to any access network / ANP. The realization of the full mobility potential will also have a great social impact.

The CBM also has the potential to kick-start the user-driven Integrated Heterogeneous Networking (IHN). The inherent consumers' ability to access whatever services from whatever networks (within whose footprints they are present) whenever they want, is already a basic form of IHN. Decision-making on choices is part of the ABC&S functionality. As IHN evolves, ABC&S-based functionality will support user-driven switching of live connections seamlessly among homogeneous or heterogeneous access networks, in ways largely transparent to the access networks themselves, referred to as 'hot' access network change (HAC). As the signaling involved is between users and the target network and not network-to-network it is a 'paid-for' service (i.e. not a network cost overhead as in network-driven

IHN). Some IHN-type decisions might be taken in collaboration with the mobile service providers (xSPs). In general, HAC-IHN will require supporting functionality at both ends of the service connection (user and xSP), e.g. through the use of the multi-homed functionality and dynamic address reconfiguration of the Mobile Stream Control Transmission Protocol (mSCTP), [O'Droma, 2008].

The CBM also facilitates user-driven IHN for asymmetric service provision, which is network-transparent. For instance the user and the mobile service provider (xSP) may 'collude' to communicate user requests through one type of access-network connection (e.g. 2G/3G) and download content requested through another access network (e.g. Wi-Fi/WiMax). In respect of this, neither access network needs to know about the existence of a part of the connection path through the other. HACs (under the control of the user, the xSP or both collaborating) may occur independently on both parts of such connections [O'Droma, 2008].

The trend from the SBM to the CBM is seen even today (Figure 3).

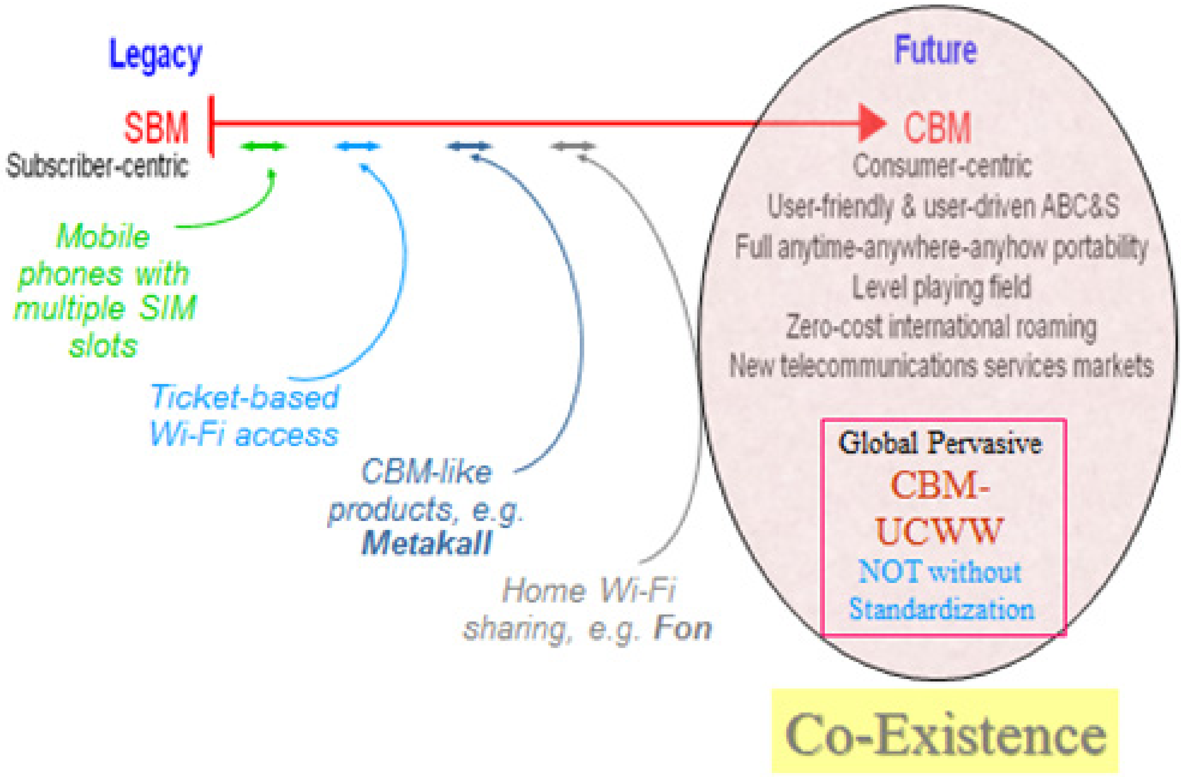

Legacy
SBM
Subscriber-centric
Mobile phones with multiple SIM slots
Ticket-based Wi-Fi access
CBM-like products, e.g. Metakall
Home Wi-Fi sharing, e.g. Fon
Future
CBM
Consumer-centric
User-friendly & user-driven ABC&S
Full anytime-anywhere-anyhow portability
Level playing field
Zero-cost international roaming
New telecommunications services markets
Global Pervasive
CBM-
UCWW
NOT without
Standardization
Co-Existence

Fig. 3. The transition trend from the SBM to the CBM

The first step, which is widely used by many users who travel a lot around the world in order to avoid high roaming charges, involves the use of dual (or even multiple) SIM active phones, which are capable of receiving calls on both (all) SIM cards. The next step is to utilize ticket/voucher-based Wi-Fi access, again for the same reason to avoid the high cost of mobile access to the Internet while roaming abroad. The third step includes CBM-like products, such as Metakall, which enables Android users to make phone calls from hot-spots operated by a range of Wi-Fi providers around the world without a need for subscription; the users just pay for the Wi-Fi service they use to make a call. Another (closer to CBM) step involves sharing of (home) Wi-Fi access with other users. A primarily example here is Fon[†] (https://fon.com)– a system of dual access wireless networks – claiming to be the largest Wi-Fi network in the world, with over eight million hotspots as at July 2013. Fon members are allowed to share a part of their Internet connection with other Fon members; otherwise users who choose not to share their Internet connection can buy Wi-Fi access passes or credit from Fon. Fon members, whose Wi-Fi hotspots are used to access the Internet by a paying customer, can receive part of the revenue.

A possible transition solution (from the SBM moving towards the CBM) could be to enable users to avail of 3P-AAA services concurrently with present (SBM) procedures. In the future, mobile phones will be bought in a shop without any binding to a particular network (provider). The user's number (i.e. a personal IPv6 address, c.f. Section 4) will be bought separately by the user and assigned to him/her (e.g. by adding it to his/her CIM card, c.f. Section 5). The key feature here is that the consumer-user will really 'own' his/her personal IPv6 address(es) and that this address will not be bound to a particular network and may be moved from one mobile device to another.

The new type of wireless communications environment UCWW, established on the CBM model, is in harmony with the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) Next Generation Networks (NGN) objectives [ITU-T, 2004]. Its focus are packet-based communications and networks (primarily IPv6). For this, it utilizes a new 'personal IPv6 address' class described further in this paper. In the UCWW, as in NGN, "service-related functions are independent from underlying transport-related technologies". The UCWW facilitates "unfettered access for users to networks and to competing service providers and/or services of their choice"; the users are not tied to any particular ANP. The UCWW also caters for "generalized mobility which will allow consistent and ubiquitous provision of services to users". Mobility in the UCWW is end-to-end controlled and executed, e.g. via a Hot Access network Change (HAC) with service session continuity, and is primarily user-driven (and also supported by the mobile service providers), and facilitated by a full number portability. Interworking with legacy networks is supported via open interfaces. For this, four new open 3P-AAA

[†] Nowadays Fon is working mostly with mobile operators, telecommunications companies, and service providers by providing global Wi-Fi access and technology solutions to them.

interfaces are defined and explained in the next section. The UCWW supports unified service characteristics for the same service as perceived by the mobile user. It also provides decoupling of service provision from the network. Furthermore, the UCWW supports a variety of identification schemes, which can be resolved to IP addresses for the purposes of routing in IP networks. The main identification scheme is based on the novel concept of the personal IPv6 address.

A high-level view of the UCWW is depicted in Figure 4.

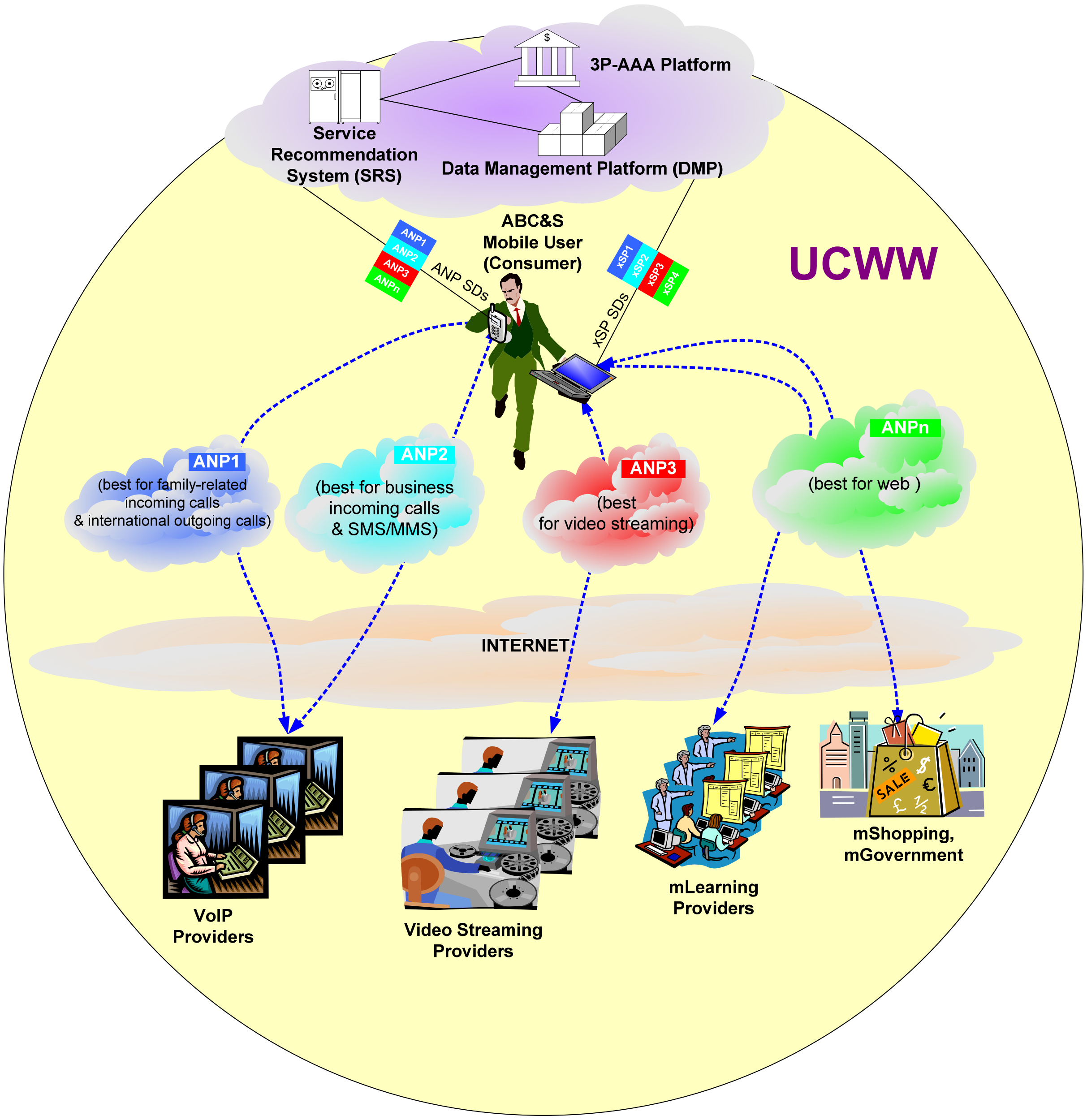

3P-AAA Platform
Service Recommendation System (SRS)
Data Management Platform (DMP)
ABC&S Mobile User (Consumer)
ANP1
ANP2
ANP3
ANPn
ANP SDs
xSP1
xSP2
xSP3
xSP4
xSP SDs
UCWW
ANP1
(best for family-related incoming calls & international outgoing calls)
ANP2
(best for business incoming calls & SMS/MMS)
ANP3
(best for video streaming)
ANPn
(best for web)
INTERNET
VoIP Providers
Video Streaming Providers
mLearning Providers
mShopping, mGovernment

Fig. 4. A high-level view of the UCWW

By utilizing a distributed cloud-based Service Recommendation System (SRS) as proposed in [Ganchev, 2015b], the 'best' service instances are found and recommended to mobile users in a highly personalized and customized way to suit each of them thus facilitating the access to those services through the 'best' available wireless connection under the ABC&S communications paradigm. Moreover, it is a true form of a user-driven ABC&S, which is facilitated and supported by the mobile service providers (xSPs). From a functional point of view, in addition to the SRS, another important UCWW infrastructural component is the Data Management Platform (DMP) [Ganchev, 2016a], which acts as a machine learning platform for turning raw data into actionable analytic dataset, i.e., user behavior profiles, including user preferences, content consumption preferences, shopping preferences, interest preferences, app usage, etc., abiding by the user-privacy principles. For this, it utilizes real-time user’s profiling algorithms and off-time data processing algorithms [Ganchev, 2016b].

Naturally new architectural entities, technical and standardization innovations, and internationally agreed protocol structures are required for a managed CBM-UCWW revolution as to support many aspects of this new concept, such as secure protocol interfaces for 3P-AAA-SPs, user identification by a tamper-resistant smart CIM card containing the user’s credit card details and providing these when needed as a ‘secure AAA ticket’, etc. These and other CBM aspects are considered in the next sections.

3. 3P-AAA

As already stated, the 3P-AAA service providers (3P-AAA-SPs) are new business entities, playing a central role in the UCWW, established on the CBM model. Through these entities, all wireless communications- and mobile services’ purchasing transactions are made. For the user, this process is accomplished by means of a smart CIM card installed on his/her mobile device. The 3P-AAA facilitates reaching the main CBM goal of separation of the administration and management of users’ AAA activity from the supply of a wireless access network service. The 3P-AAA-SPs are (access) network-independent, autonomous, and trusted business entities. This is to prevent their unfair access, in the role of an ANP, to a very wide database of consumers and xSP market information, which could disadvantage other ANPs. This is a strong distinction between the CBM and the SBM with significant socio-economic implications. It may require international regulation, though more likely with time consumer and competition dynamics will make this unnecessary [O’Droma, 2008].

Analogous to the credit-card payment systems, each service charge incurred by a user may be paid indirectly through the user’s 3P-AAA-SP, who will periodically send out itemized bills to him/her. This will create also new business development opportunities through the expansion into all areas of purchasing via this smart CIM card and the development of new “mobile money” / “wireless wallet” mobile apps for payment. Examples of potentially suitable 3P-AAA-SPs are financial institutions, such as present-day credit-card companies.

Some proposal details on security, the functional model, and signalling protocols for the 3P-AAA architecture are presented below.

The 3P-AAA interface infrastructure's and signaling protocols' standardization program to enable global provision of 3P-AAA services is outlined in [O'Droma, 2010]. Standards proposed for agreement should respect the need for these services to be scalable, hierarchical, and cognizant. Such attributes may be seen in global 3P-AAA service solutions where service providers deploy their AAA servers regionally, in multiple hierarchical layers, reflecting the dimensions and characteristics of their customer bases. Service to customers may also be improved, e.g., better response times achieved, by porting a copy of a customer's data to the AAA server in the region closest to where a customer is at the moment.

Figure 5 presents a schematic of the key features of the 3P-AAA functional model. In addition to the third-party aspect of the AAA provision, another novel element here is the installation of an AAA client directly on the mobile device. This is a radical distinction from the traditional Diameter/COPS models. Operationally-wise, a smart CIM card (e.g. based on the 'Java card' technology [Oracle, 2015]), inserted into the mobile device, could carry the 3P-AAA client application for AAA communication with various service providers. The AAA servers in the ANP and xSP domains also have 3P-AAA clients for communication with the 3P-AAA-SPs' servers, e.g. for the exchange of accounting information, and charging and billing (C&B) information for vendor transactions to consumers.

The 3P-AAA functional model is based on the following four interfaces, all new to the wireless communications world:

(a) User↔ANP/xSP;

(b) User↔3P-AAA-SP;

(c) ANP/xSP↔3P-AAA-SP;

(d) 3P-AAA-SP_x↔3P-AAA-SP_y.

Corresponding to foreseeable major market sectors, three specialized 3P-AAA-SP classes are posited in [O'Droma, 2010], namely class A for ANPs, class B for xSPs and VASPs, and class C for consumers. It is not intended with this division to exclude other forms or even that a single 3P-AAA-SP would cater for all three markets. The advantage of having different classes of 3P-AAA-SP is that each of them can focus only on one group of service functions so that these functions can be made much more sophisticated. Also with establishing such classes any consequent effects on the new interface protocols may be more easily handled. This specialization option implicates the requirement for a signaling protocol for interaction between these types of 3P-AAA-SP. For this, an Inter-3P-AAA-SP signaling protocol is required to operate over the ***d*** interface.

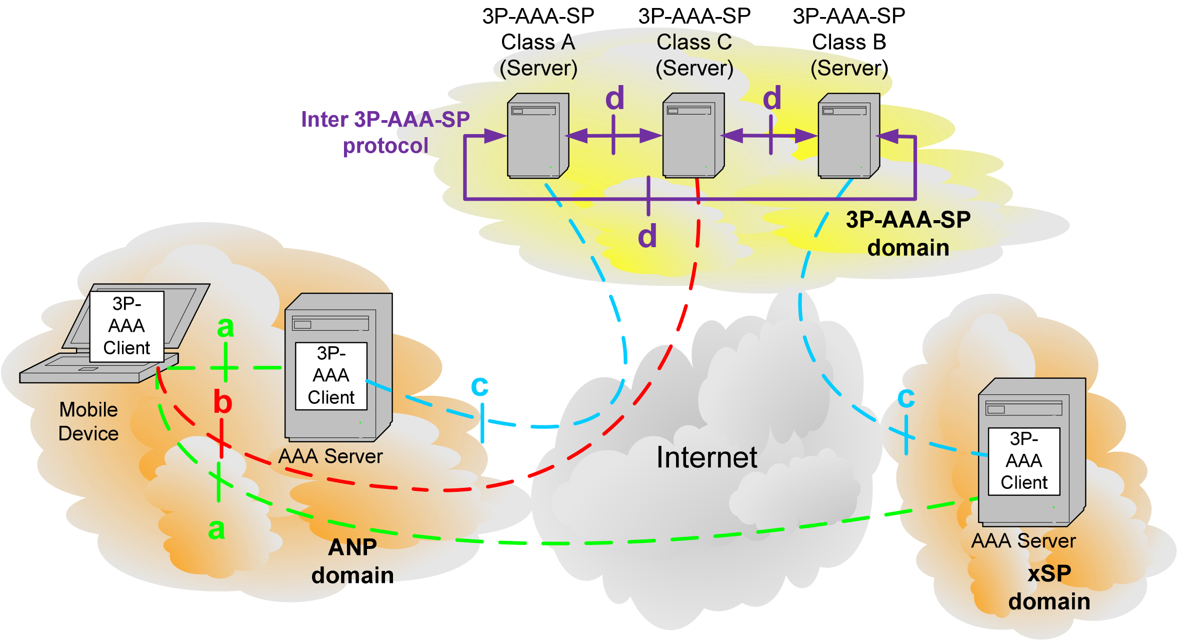


Fig. 5. The 3P-AAA functional model schematic (with four new application-layer interfaces ***a***, ***b***, ***c***, ***d***).

There will be similarities but also distinctions in the services provided within each class. For ANPs, for instance, services will include accounts and related AAA policies, C&B policies, pricing and rating functions, charging detail records generation, account balances, and the like. For consumers (besides accounts), these may include various types of credit top-up services, billing system configuration functionality, functionalities to enable customer-retention discount and promotional schemes, user-definable account format and layout, etc.

On the newly defined interfaces, the existing Internet Engineering Task Force (IETF) Diameter protocol [Calhoun, 2003] has suitable attributes for carrying 3P-AAA signaling. Being conceived for the SBM environment, however, some adjustments for 3P-AAA will be required. One potential solution is to extend its base protocol so as to support 3P-AAA functionality via the addition of new commands and/or attribute value pairs (AVP); another is to define a new 3P-AAA signaling application. The latter seems more attractive standardization route because exploiting the Diameter design, whereby it accepts new autonomous applications which run on its core, has the advantage of not constraining the Diameter core from evolving independently [O'Droma, 2010].

Through standardized protocols, the 3P-AAA client on the user's mobile device interacts with AAA servers of the ANPs and xSPs for mutual authentication and exchange of security credentials. A part of these standardized protocols will be the signaling to establish authentication securely prior to any service purchase. An authentication scheme, based on the ITU-T's X.509 recommendation for a public key infrastructure (PKI) [ITU-T, 2012], can support strong secure mutual authentication and trusted relationship establishment between communicating parties with a minimum number of protocol exchanges.

An example of the consequences of this kind of methodology, being applied to the 3P-AAA infrastructure, is an amendment proposed in [O'Droma, 2010] to the ITU-T's authentication architecture for interworking in NGN [ITU-T, 2008] which to enable user-driven IHN. Figure 6 represents the ITU-T's graphical illustration of an NGN authentication architecture for interworking among heterogeneous wireless networks operating within the SBM. Its objective is to enable a subscriber of one (home) network, e.g., a 3G cellular network, to gain wireless access services as a roamer from another heterogeneous network, e.g., a WLAN or WiMax network, with payment executed through the home network. The approach also may form a basis for subscriber-transparent network-driven handover while roaming among collaborating heterogeneous networks. It uses a four-layer architecture, with the user equipment (UE) at the bottom. The network attachment control function entities are the authenticator (AM-FE), acting as an AAA client, and the home-ANP's AAA server (TUP-FE/TAA-FE) positioned at the third and fourth layers, respectively. The second layer (AR-FE in the access network) acts as an enforcement point filtering packets and allowing through only packets exchanged for initial authentication or subsequently authenticated data packets. The key communication to allow roaming on a heterogeneous network is on the 'roaming interface', (marked 'R' in Figure 6) between the AAA servers in the different network domains.

The proposed modifications of this architecture for the UCWW environment are overlaid on this ITU-T illustration. In the UCWW, the 'home network' attribute no longer applies to access networks. Also the roaming interfaces 'R' are not required. Instead 3P-AAA server entities are present, with which the network-specific AAA servers communicate over standardized 3P-AAA interfaces of type ***c***. Similar type interfaces are needed between 3P-AAA servers and the service-specific AAA servers (SAA-FE). In addition, the AAA client is shifted from the network to the mobile device (UE), and its communication with the ANP's AAA server and 3P-AAA server is performed over the proposed standardized 3P-AAA interfaces of type ***a*** and ***b***, respectively. The balance of the heterogeneous networking decision-making power is now much more in the hands of mobile users and away from networks.

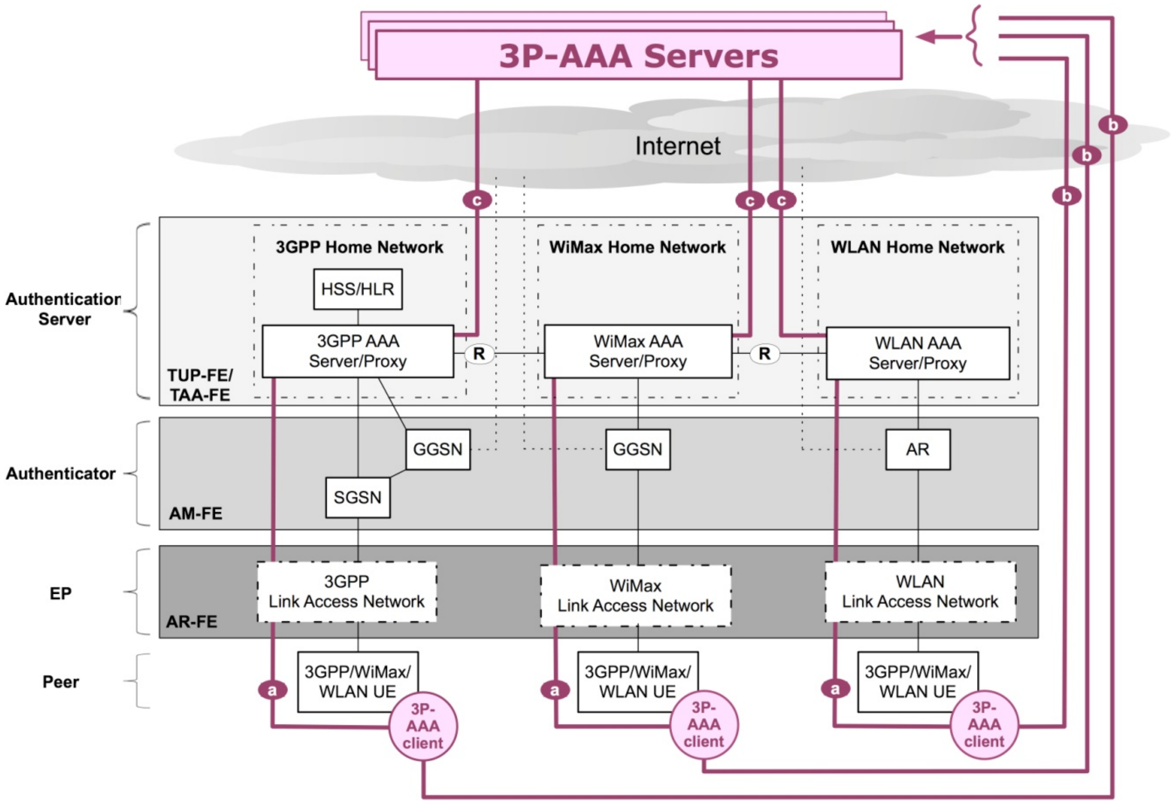


Fig. 6. The ITU-T’s SBM authentication architecture for interworking in NGN

and the proposed modification (in purple color) for the UCWW, established on the CBM.

The signaling between 3P-AAA servers and local AAA servers of ANPs (and xSPs) could lead to significant network traffic. This would be the case if the charging and billing (C&B) implementation includes a requirement for continuous processing of the frequently clocked records coming from individual charging functional entities in order to calculate the correct service charge. This is a typical implementation for C&B of phone calls, and other non-flat-rate services, in the SBM environment today. To address this, the concept of a C&B agent could be utilized. Downloaded in advance from the 3P-AAA-SP and deployed in the metering domain of the ANP (or xSP), this agent would perform all associated C&B functions there. For this, the agent would come with a budget for the service to be supplied to the consumer and any other relevant consumer-account details. This agent would have the functionality to manage the budget, e.g., expending it in response to the provider’s (ANP or xSP) metering triggers, sending budget replenish requests to the 3P-AAA server when a budget depletion threshold is crossed, and at the end of the service session informing the 3P-AAA server of the total charge, [O'Droma, 2010]. More aspects of the corresponding C&B, including details of evaluation of possible 3P-AAA policy-based accounting models, the possible authorization framework, the proposed generic third-party C&B (3P-C&B) architecture along with supporting protocol candidates, the corresponding rating scenarios for different 3P-AAA-SP classes involved, etc., are presented in [Jakab, 2014]. For instance, the protocol analysis conducted there confirms that for the 3P-AAA infrastructure some extensions of the conventional AAA protocol (e.g. Diameter) will be required, e.g. for Network Access Server (NAS), mobility support, resource brokering, etc.

The novel 3P-C&B approach has the potential of creating an innovative environment for service creation with the following strengths [Jakab, 2009]:

- Providers (ANP, xSP, VASP) do not need to invest in their own C&B system;
- Providers can focus better on their services;
- Providers get the C&B system for free;
- Newly created services (access network communications services or mobile services) are automatically exposed to consumers after their registration with the 3P-AAA-SP;
- Delivery of a 'fair 5G system':
    - The consumer chooses which provider (ANP/xSP/VASP) and which service instance s/he is going to use (so each provider has equal chance for success!);
    - The consumer can freely seek for 'value for money' services;
- Creation of sophisticated C&B systems:
    - 3P-AAA-SPs can invest in their charging services (for new charging schemes or flexible charging solutions) and these will automatically be available to each provider, which would certainly raise more interest and bring new clients.

4. New 'Personal Address' Scheme

For the proposed user address ownership, standardization of a separate class of globally-significant, network-independent 'personal' IPv6 (PIPv6) addresses, as proposed in [Ganchev, 2007], is needed. The PIPv6 address is a static, permanent, and unique address, which is managed and allocated by a global address supplier. Its uniqueness will eliminate the need for duplicated address detection, which is compulsory in IPv6 networks with stateless address auto-configuration (SLAAC).

This new PIPv6 address will enable real consumer-number ownership and full 'anywhere-anytime-anyhow' portability for future generations of mobile users empowered to opt out of their long-term subscriptions with access network providers, and use advertised communication services from any consumer-centric wireless access network present to them. The PIPv6 address can also give more flexibility to set up and operate Wireless Networks of Moving Objects (WiNeMO) [Ganchev, 2014a] because a node (object) can use the same address (identity) in every case and in any communication scenario. It could be used as a long-term identity solution that can prevent impersonation, and Sybil, whitewashing and similar attacks in WiNeMO, and be useful in schemes to deter other types of security attacks.

A new IPv6 address class should be identified for this new PIPv6 address by appropriately assigned *Class Prefix*. Figure 7 shows a possible format, with the space including this field and three other fields, described below. A further small *version* field may also be advisable to allow greater restructuring flexibility in the future.

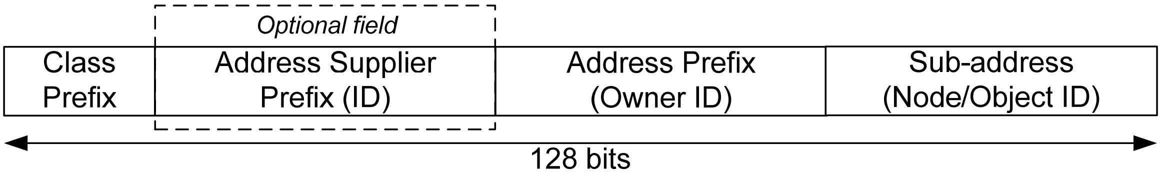

Optional field
Class Prefix
Address Supplier Prefix (ID)
Address Prefix (Owner ID)
Sub-address (Node/Object ID)
128 bits

Fig. 7. The format of the new personal IPv6 (PIPv6) address.

The *Address Prefix* is the primary field in the PIPv6 address which could be used to identify the owner (user) of the address. Having the length of the *Owner ID* ranging from 34 to 37 bits will allow addressing of 17 to 137 billion owners. This may seem plenty in a world population context of 7 billion. However, perhaps a longer length, such as 40 bits, would be advisable to increase the duration before a long-lease address automatically reverts to the pool, and to reduce the cost (e.g., of enforcing leases), stress or necessity on returning addresses over a few generations. It is probably important to be generous on this number as the whole PIPv6 concept is to serve the goal of personal addressing and having an unlimited range (or as near as seems like that) is in the best interests of that goal. An additional *Sub-address* field is owner/user assignable and could be used by the owner for a range of sub-addresses (each for use in a separate transition scenario or developing wireless scenario). The assignable sub-address part may also be used as a *Node/Object ID* to facilitate its smooth participation in Mobile Ad hoc NETworks (MANETs), Vehicular Ad hoc NETworks (VANETs), and other WiNeMO types. The length of this field should be sufficiently large to allow addressing of hundreds of nodes/objects belonging to the same owner. For instance, allowance can be made for narrowcast addresses which may find use in corporations and various community and social groupings.

Key to any network-independent personal address is the prevention of duplicates, whether by accident or (malicious) design. A second issue is the eventual return of unused addresses or addresses whose use has ceased or become defunct. In the case of the PIPv6 address proposal, this could be achieved by a centralized purchased scheme through authorized address suppliers, each of which owns a portion/subset of this new IP address class' space and is identified by an optional *Address Supplier ID* field and/or by characteristics in the *Owner ID* field in the address. The selling of PIPv6 addresses within a 'renewable lease-based' system would also facilitate unused or defunct addresses being returned to the pool of available addresses [Ganchev, 2014b].

Obtaining PIPv6 addresses would be a commercial transaction. In addition, as there is no reason why owners might not engage in address trading, the commercial legal arrangements should allow for this, e.g. ownership should be legally verifiable and transferable without difficulty. Perhaps this responsibility would ultimately fall to an Internet Assigned Numbers Authority (IANA) / Internet Corporation for Assigned Names and Numbers (ICANN)-type organization. Address trading would also incentivize use or return of addresses. There would be privacy concerns with this permanent PIPv6 address employed by users for node/object identification and addressing, authentication, authorization and network access admission. These reflect on possible compromise of privacy related to the potential for tracking of, and gathering statistics about, a user/node/object as s/he/it moves through different locations. However, some of the existing mechanisms for privacy protection may still be used in this case, e.g., encrypting the traffic at different communication layers, use of temporary or changing "pseudonyms" as identifiers, etc., [Ganchev, 2014b].

There is also a need for this new PIPv6 address to be securely 'locked' to enable the user/node/object to be uniquely identified and authenticated during communication. This is a key attribute. It could be achieved by embedding the PIPv6 address into a X.509 public-key digital certificate. The ITU-T's X.509 authentication framework [ITU-T, 2012] defines a good model for strong secure authentication with a minimum number of exchanges. The authentication is performed through simple automatic exchange of X.509 digital certificates between communication parties (network nodes, objects, entities, etc.). It seems reasonable to employ the three-way option for mutual authentication, as it does not require the communication parties to have synchronized clocks. The exchange of certificates will enable trusted relationship and secure payment of (micro) transactions in the UCWW.

The extensions defined in version 3 of the X.509 standard (X.509v3) provide methods for associating additional attributes to carry information unique to the owner of the certificate. In particular, the *Subject Unique ID* field (Figure 8), which allows additional identities –e.g. e-mail address, Domain Name System (DNS) name, IP address, Uniform Resource Identifier (URI), etc.– to be bound to the owner, can accommodate the proposed PIPv6 address. This, however, must be clearly marked as a critical X.509v3 extension in order to be used in a general context [ITU-T, 2012]. Because the *Subject Unique ID* is definitively bound to the public key, all parts of it (including the PIPv6 address) can be verified by the corresponding certificate authority (CA).

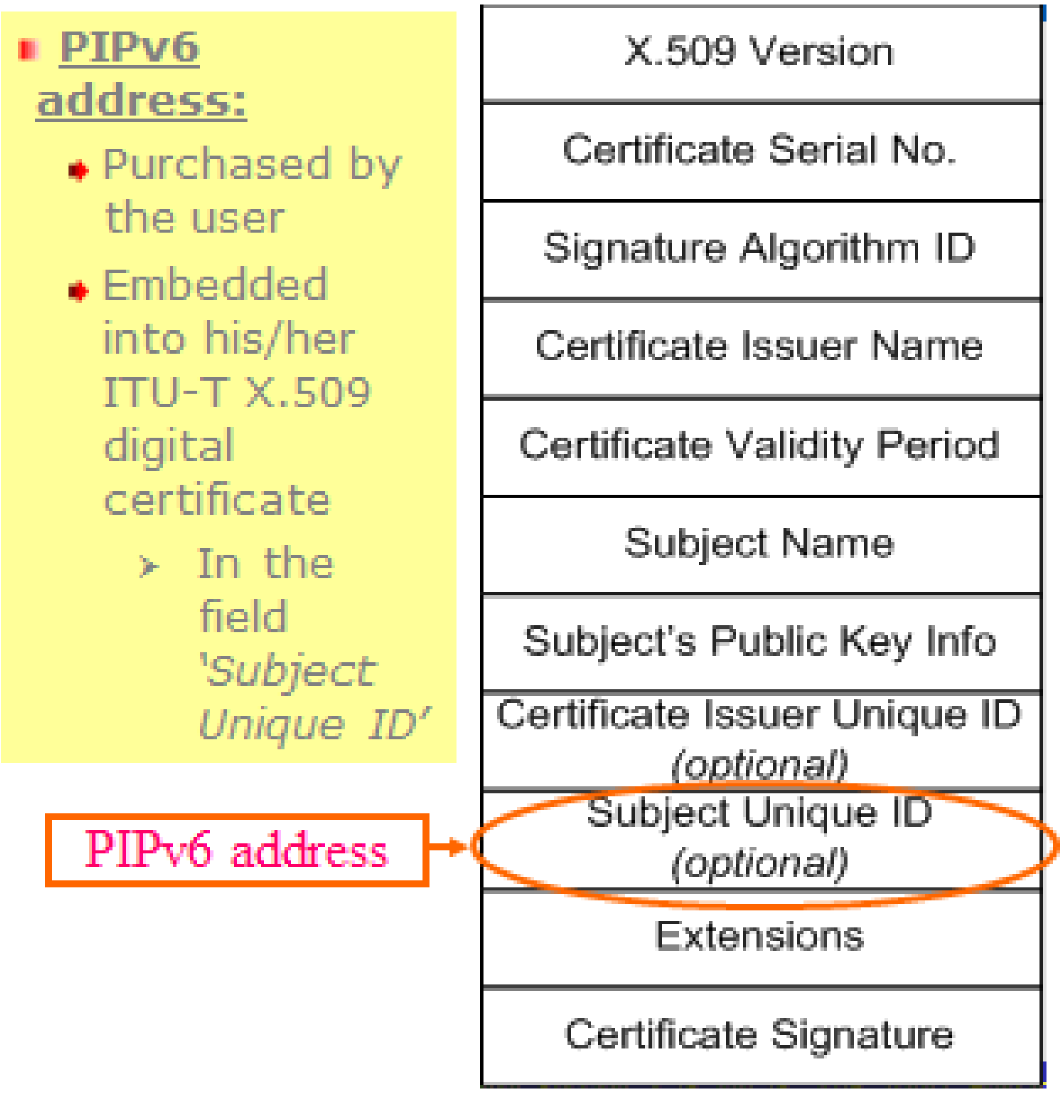

PIPv6 address:
Purchased by the user
Embedded into his/her ITU-T X.509 digital certificate
In the field 'Subject Unique ID'
PIPv6 address
X.509 Version
Certificate Serial No.
Signature Algorithm ID
Certificate Issuer Name
Certificate Validity Period
Subject Name
Subject's Public Key Info
Certificate Issuer Unique ID (optional)
Subject Unique ID (optional)
Extensions
Certificate Signature

Fig. 8. The PIPv6 address, embedded in the user's X.509 digital certificate.

A generic WiNeMO communication scenario using the PIPv6 address is depicted in Figure 9. The scenario imagines a mobile node (object) seeking and finding a gateway (GTW) among or through those mobile nodes (MNs) available to it as relays either directly or through other mobile nodes in a WiNeMO network. The GTW is defined as an access point to connect directly to the Internet and through it – to a particular correspondent node (CN). First, a mutual authentication procedure is executed between the object and all other supporting relay nodes in this scenario, including the GTW. This being successfully completed, the GTW decides to allow (or not) the object to use its Internet connection for a particular period of time. Then the GTW accepts the PIPv6 address supplied by the object and stores it in its Network Address Translation (NAT) table along with the corresponding IPv4 address to be used for this new Internet session for the duration of communication between the object and CN. Then GTW confirms to the object that it may start using the Internet for communication with CN. After that, following the standard NAT IPv6-to-IPv4 (NAT64) procedure, each IPv6 packet originating from the object will carry its PIPv6 address in the *Source Address* field. When this packet reaches the GTW, the PIPv6 address of the object (used only locally) will be translated into the public IPv4 address allocated to the GTW for global routing on the Internet. In other words, as the IP traffic passes from this WiNeMO to the Internet, the GTW translates 'on the fly' the source address in each packet from the PIPv6 address of the particular object engaged in communication to (one of) its own public IPv4 address(es). The reverse address translation is performed in the opposite direction of communication.

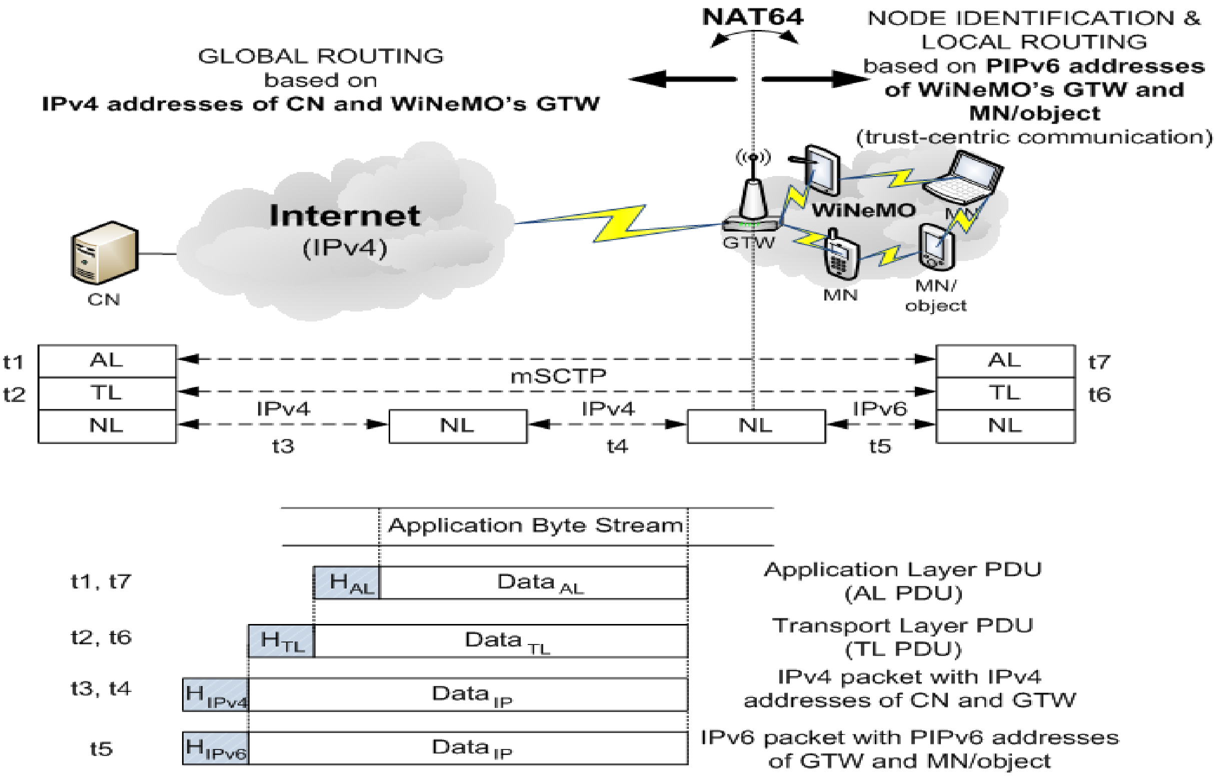


Fig. 9. A generic WiNeMO communication scenario using the PIPv6 address.

5. Smart CIM Card

This new type of card is proposed in [O'Droma, 2007] for the mobile users so as to behave as consumers in the UCWW with whatever mobile device chosen, i.e. to obtain and securely pay for services from any ANP/xSP, anywhere-anytime-anyhow, thus achieving advanced user mobility. With CBM and through their CIM card, consumer-users, wherever they are, would always appear as 'local users' to whatever networks they roam in. Implicit in being a 'local user' is that roaming charges will disappear! Through their universal X.509-based smart CIM cards, consumers would own their personal globally significant, network-independent PIPv6 address(es). By means of relevant CAs' public key infrastructures (PKIs), the validity of the certificates of all parties to a transaction may be mutually checked as required.

The CIM card could be developed by using the 'Java Card' technology [Oracle, 2015], which provides highly secure, market-proven, and widely deployed open-platform architecture for the rapid development and deployment of smart-card applications meeting the real-world requirements of secure system operations. The Java-based CIM card may typically be a plastic card containing an embedded chip. It will enable the client applications to run on a single virtual machine, in order to maintain the user profiles, credit card information, PIPv6 address(es), 3P-AAA data, X.509 certification, etc. As these applications will be required to communicate with each other using shared interface objects (SIO), a firewall must be defined for each application to provide application-level security. A sample CIM card architecture is presented in [Ganchev, 2007] and depicted on Figure 10.

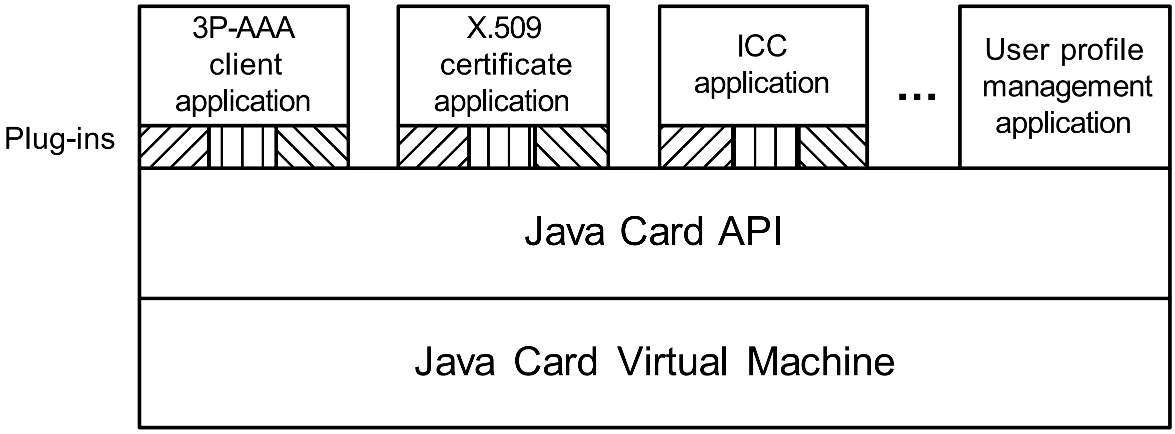

3P-AAA client application
X.509 certificate application
ICC application
...
User profile management application
Plug-ins
Java Card API
Java Card Virtual Machine

Fig. 10. A sample CIM card structure

The multi-application processor CIM card inserted in the mobile device will have one or more 3P-AAA application clients installed. This devolution of application programs and processing power to the CIM is a significant change from the legacy SIM card operations. Simultaneous accounts with different 3P-AAA-SPs will be possible. CIM cards, for instance, could come with generic 3P-AAA clients pre-installed and several free spaces on the card chip leasable to specific 3P-AAA-SPs for installing (and upgrading) their own specific 3P-AAA client, designated for that consumer.

Different other applications/applets could be deployed on the CIM card, e.g. an application for managing consumer's X.509 certificates, an ICC application for facilitating the incoming call connection (ICC) service provision, an application for managing the user profile(s), etc. Additionally installed plug-ins will allow further personalization of each application, e.g. in the case of 3P-AAA the user may install a separate plug-in for each individual 3P-AAA-SP with whom s/he has an agreement for AAA and C&B of services (the use of each particular 3P-AAA-SP is activated depending on the current user context as specified in the user profile). The commercial relation between the CIM card issuer and the application provider is independent of the platform technology, ensuring a really open market space. For instance in the 3P-AAA case, the business agreements are between the CIM card issuer and the 3P-AAA application provider, where the issuer can specify the extent of its responsibility for the overall card security and the 3P-AAA application provider can assume its own responsibility for the secure 3P-AAA operation of its in-card business logic implemented in the loaded 3P-AAA client application [Ganchev, 2007].

The Java Card platform provides a secure execution environment with a firewall between different applications on the same card. Each application can encapsulate sensitive data and algorithms within objects, which have provable behavior and increased security. Further security enhancements, such as transaction atomicity and cryptographic classes, are also provided. In addition the dynamic download capability of the card ensures that applications can be securely managed, i.e. tamper-proof downloaded, installed, configured, updated, and removed after the card has been issued.

The Java Card Virtual Machine (JCVM) separates applications from the underlying hardware and operating system. "Split virtual machine" architecture is used: one part is executed on the user's mobile device, preparing the code for execution in the other part of the virtual machine, on the card. The split JCVM design is intended to reduce the size of the applet image downloaded to the card and to minimize run-time memory requirements [Oracle, 2015]. A standardized API provides a uniform interface to applications and extension Java packages.

The approach towards the UCWW personalized and multi-serving client applications is seeking designs on a smart programmable handheld mobile devices to interoperate seamlessly with the CIM. Given the expected dominance (greater than 50%) of the Android operating system, the development of a client application working within a Google Android environment is primarily targeted [Ganchev, 2015a]. Consistent with this is also the integration of a SIMAlliance Open Mobile API specification [SIMAlliance, 2014] into the Android platform to enable mobile devices to communicate with secure elements in the CIM.

Developing the CIM card as a **virtual card** is another promising direction which deserves better attention in the future.

6. Conclusion

Technical foundations for an effective techno-business model which will make the evolution to a truly Always Best Connected and best Served (ABC&S) fifth generation (5G) wireless world possible have been addressed in this paper. The flaws in the current Subscriber-Based techno-business Model (SBM) for this evolution have been highlighted. An argument for a Consumer-Based techno-business Model (CBM) has been made and a view on the changes and innovations needing to be made to the network and protocol technological structure to achieve this has been put forward. This includes an infrastructural re-think on the way Authentication, Authorization and Accounting (AAA) service is supplied, proposing the creation of a third-party AAA service provider entity (3P-AAA-SP), together with a number of new technological supports requiring global standardization, including a novel personal IPv6 (PIPv6) address mechanism and a new smart Consumer Identity Module (CIM) card utilizing X.509v3 digital certificate security. The new globally significant, network-independent PIPv6 address will enable real number ownership and full ‘anywhere-anytime-anyhow’ portability. It has been proposed and envisaged that in future generations of wireless networks, nodes (objects) will have a unique PIPv6 address, which may serve also as a means of long-term node identity in the network.

While initially the CBM infrastructure may seem to threaten the establish large subscriber-based access network provider (ANP) market share, it has been argued rather that it would greatly open, and ease entry into, the ANP- and mobile service provider (xSP) markets for new entrants, for ‘disruptive’ and creative technologies, and stimulating competition and new and improved services, and all in a way that will be of benefit to all stakeholders.

Mobile users today need ever more choice and customization in the provision of (mobile) services with more flexible service delivery and an ability to move/migrate quickly to more competitive providers who can provide better price/performance options, a wider selection of service offerings, etc. The Ubiquitous Consumer Wireless World (UCWW) is a creative proposal requiring the implementation of the CBM model for wireless communications. This, in turn, requires the underpinning of some strategic standardization as highlighted in the paper. Once the new standardized elements are in place, the UCWW will begin to take shape and grow along an evolutionary path (as happened with, and in parallel with, the existing wireless world founded on the SBM model) yielding social, economic and policy benefits for users, ANPs (mobile operators), hardware and software suppliers, the full range of mobile service providers and new business entities, such as the cloud service providers. The novel 3P-AAA-SP concept seems especially attractive for the emerging inter-cloud service providers' business.

Acknowledgements

This work is funded and supported by the Telecommunications Research Centre (TRC), University of Limerick, Ireland and by the IT15-FMIIT-004 project of the Scientific Fund of the Plovdiv University "Paisii Hilendarski", Bulgaria.

The author wishes to specially thank the TRC Director, Dr. Máirtín O'Droma, for the fruitful discussions and inspiring thoughts on the subject through many years.

Bibliography

[Calhoun, 2003] P. Calhoun et al., "Diameter Base Protocol", IETF RFC 3588, 2003.

[Ganchev, 2007] I. Ganchev and M. O'Droma. "New personal IPv6 address scheme and universal CIM card for UCWW". Proc. 7th Int. Conf. on Intelligent Transport Systems Telecommunications (ITST 2007), Pp. 381-386. 6-8 June 2007, Sophia Antipolis, France. IEEE CN-07EX1765.

[Ganchev, 2014a] I. Ganchev, M. Curado, A. Kassler (Eds.): Wireless Networking for Moving Objects - Protocols, Architectures, Tools, Services and Applications, LNCS 8611, pp. 301. Springer International Publishing, Switzerland. September 2014. ISBN: 978-3-319-10833-9. DOI: 10.1007/978-3-319-10834-6.

[Ganchev, 2014b] I. Ganchev and M. O'Droma. 2014. "A New Techno-Business Model based on a Personal IPv6 Address for Wireless Networks of Moving Objects". In: Wireless Networking for Moving Objects - Protocols, Architectures, Tools, Services and Applications. I. Ganchev, M. Curado, A. Kassler (Eds.). Springer International Publishing, Switzerland. September. ISBN: 978-3-319-10833-9. Pp. 3-13. DOI: 10.1007/978-3-319-10834-6.

[Ganchev, 2015a] I. Ganchev, Z. Ji, M. O'Droma, C. Dai. 2015. "A CIM System for Use in the UCWW". Proc. of the 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC 2015). Pp. 72-75, 17-19 September, Xi'an, China. ISBN 978-1-4673-9200-6/15. DOI 10.1109/CyberC.2015.63.

[Ganchev, 2015b] I. Ganchev, Z. Ji, M. O'Droma. 2015. "A Distributed Cloud-based Service Recommendation System". Proc. of the 2015 International Conference on Computing and Network Communications (CoCoNet'15). Pp. 212-215. 16-19 December, Trivandrum, India. ISBN: 978-1-4673-7309-8/15. DOI: 10.1109/CoCoNet.2015.7411189. Library of Congress: CFP15C74-USB.

[Ganchev, 2016a] I. Ganchev, Z. Ji, M. O'Droma. “The Creation of a Data Management Platform for Use in the UCWW”. Proc. of 2016 SAI Computing Conference. Pp. 585-588. 13-15 July 2016. London, UK. ISBN: 978-1-4673-8460-5/16.

[Ganchev, 2016b] I. Ganchev, Z. Ji, M. O'Droma. “A Conceptual Framework for Building a Mobile Services' Recommendation Engine”. Proc. of the IEEE International Conference 'Intelligent Systems' (IEEE IS 2016). Pp. x1-x5. 4-6 September 2016. Sofia, Bulgaria.

[ITU-T, 2004] ITU-T Recommendation Y.2001: General overview of NGN. In Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks (Next Generation Networks – Frameworks and Functional Architecture Models). Dec. 2004.

[ITU-T, 2008] ITU-T Draft Recommendation Q.3202.1 (Q.nacf.auth1), “Authentication Protocols based on EAP-AKA for Interworking among 3GPP, WiMax, and WLAN in NGN”, 2008.

[ITU-T, 2012] ITU-T Recommendation X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. In Series X: Data Networks, Open System Communications and Security Directory. Oct. 2012.

[Jakab, 2009] J. Jakab. “New Charging and Billing Models and Mechanisms for the Ubiquitous Consumer Wireless World (UCWW)”. Transfer Report (from Masters to PhD). University of Limerick, Ireland. 2009.

[Jakab, 2014] J. Jakab, I. Ganchev, M. O’Droma. “Third-party AAA and corresponding Charging and Billing of Services”, Presented at the COST IC1304 3rd MCM on "Autonomous Control for a Reliable Internet of Services (ACROSS)". Larnaca, Cyprus, 23-24 October 2014.

[O’Droma, 2004a] M. O'Droma and I. Ganchev. “New Access Network Techno-Business Model for 4GWW”. Proc. of 4th ANWIRE International Workshop on Wireless Internet and Reconfigurability (held in conjunction with the 3rd IFIP-TC6 Networking Conference), Pp. 75-81. 14 May 2004. Athens, Greece.

[O’Droma, 2004b] M. O’Droma and I. Ganchev. 2004. “Techno-Business Models for 4G” (invited paper), Proc. of the International Forum on 4th Generation Mobile Communications, Pp. 3.5.1-30, 20-21 May, King’s College London, London.

[O’Droma, 2007] M. O’Droma and I. Ganchev. “Towards a Ubiquitous Consumer Wireless World”. IEEE Wireless Communications, Feb. 2007, Pp. 2-13. ISSN: 1536-1284.

[O’Droma, 2008] M. O’Droma and I. Ganchev. “Strategic Innovations through NGN Standardisation for a Ubiquitous Consumer Wireless World”. Proc. of the 1st ITU-T Kaleidoscope Academic Conference “Innovations in NGN”. Pp. 135-142, 12-13 May 2008. Geneva, Switzerland. ISBN 92-61-12441-0. DOI 10.1109/KINGN.2008.4542259. (Best Paper Award Nomination)

[O'Droma, 2010] M. O'Droma and I. Ganchev. "The Creation of a Ubiquitous Consumer Wireless World through Strategic ITU-T Standardization" (invited paper). IEEE Communications Magazine, Vol. 48, Issue 10, Pp. 158-165. October 2010. ISSN: 0163-6804. DOI: 10.1109/MCOM.2010.5594691.

[Oracle, 2015] Specifications for the Java Card 3 Platform Version 3.0.5, Classic Edition. Oracle Release Notes. October 2015. https://docs.oracle.com/javacard/3.0.5/JCSRN.pdf

[SIMAlliance, 2014] "Open Mobile API specification: V2.05". SIMAlliance. February 2014. http://simalliance.org/wp-content/uploads/2015/03/SIMalliance_OpenMobileAPI2_05_release-Feb143.pdf

Author's Information

***Ivan Ganchev** – DipEng (summa cum laude), PhD, SMIEEE, ITU-T (Invited Expert), IJTMCC Regional Editor (Europe).*

TRC Deputy Director, University of Limerick, Limerick, Ireland & Associate Professor, Plovdiv University "Paisii Hilendarski", Bulgaria; e-mail: Ivan.Ganchev@ul.ie

Major Fields of Scientific Research: novel telecommunications paradigms, future networks and services, smart ubiquitous networking, context-aware networking, mobile cloud computing, Internet of Things (IoT), Internet of Services (IoS), Ambient Assisted Living (AAL), Enhanced Living Environments (ELE), trust management, Internet tomography, mHealth and mLearning ICT solutions.