User-centric networking: bringing the Home Network to the Core

Rute Sofia*

COPELABS, University Lusófona, Lisbon, Portugal
rute.sofia@ulusofona.pt

Abstract. This paper goes over the concept of User-centric networking, as a paradigm for networking architectures usually located in the Customer Premises, and which is steadily changing the way the Internet has been devised. Such change is due to the fact that the Internet end-user is empowered due to novel approaches such as software defined networking, thus being in control of functionality that so far was restricted to be placed in the core and access regions of networks. Such change introduces the need to revisit home networking, and from an end-to-end perspective, to introduce new concepts and technology into the networking functionality. The paper presents a user-centric model and its functional blocks, and describes the architectural example that has been conceived, implemented, and validated in the context of the European project ULOOP - User-centric Wireless Local Loop.

1 Introduction

Today's end-user is connected to the Internet by means of a variety of broadband access technologies that usually do not directly reach the *end-user equipment (UE)*. Rather, this final segment of the local-loop (last mile) is provided by a number of short-range technologies, among which *Wireless Fidelity (Wi-Fi)* is the de-facto solution. The growing popularity of Wi-Fi as a complementary technology to Internet broadband access is not due to its extraordinary technical aspects. Instead, it relates to its low-cost and worldwide availability, to the ease of use, and to the high interoperability that it is capable of sustaining, when interfacing with Internet broadband access technologies. Having the last-hop of the Internet (towards the user) based on Wi-Fi comes with a price, namely, bottlenecks. Nevertheless, there are clear advantages in terms of Internet wholesale models, as each residential household becomes a Wi-Fi hotspot that at same instant in time is underused.

Due to such deployment as well as due to the introduction of new paradigms such as *Software Defined Networking (SDN)* Wi-Fi is giving rise to new models of Internet connectivity. In these new Internet access models, the end-user is one of the key pieces and ceases to simply be a consumer of Internet services (be it

* COPELABS, University Lusófona, Building U First Floor, Campo Grande 388, 1749-024 Lisboa.

connectivity or content), to become an active hop of the connectivity distribution chain.

User-centric networking (UCN) [19,1] explores concepts to allow user-centric wireless local-loops to form autonomously. The term user-centric in this context is meant to express a community model that extends the reach of a high debit, multi-access broadband backbone from different perspectives (technical, business model). Such a model is expected to be beneficial both from an end-to-end and from an access perspective, given that it allows expanding high debit reach in a seamless, cooperative, and low-cost manner. Moreover, UCN follows an evolutionary path in the context of future Internet architectural design, by building on existing work related to the recent trend of *Do-it-Yourself Networks (DIYN)*. Hence, a fundamental difference between such work and previous contributions on ad-hoc or mesh networking relates to the fact that UCN assumes that an infrastructure providing Internet access to specific locations is widely available, and users are simply willing to expand such infrastructure by exchanging some resources (networking resources, services). UCNs are also based on the notion that trust circles can assist in cooperative behavior involving both the access and the end-user.

These aspects empower the user role as an active element of networking given that i) the user becomes a producer/provider of specific services; ii) the user device is part of the network. It should be noticed that this is an aspect that goes against the Internet end-to-end principle, which describes a clear functional splitting between end-systems and the network. UCNs therefore pose challenges that are worth to be analyzed from an operational network perspective, as UCNs are supported also by devices residing in the *Customer Premises (CP)* and for the largest majority, in residential (home network) scenarios. Hence, future Internet models have to integrate properties that allow nomadic end-user experience for any application across multi-access or single-access networks, assuming that one or more operators are involved. UCNs subvert the current notion of Internet architectural design, as they impact the Internet wholesale model chain, by empowering the end-user as an active stakeholder in the core network. Functionality that usually resides in the core network becomes more useful if placed closer to the Internet end-user.

From a business perspective, wireless local-loops that are built mainly based upon an Internet stakeholder willingness to cooperate should be a starting point to revisit current business models for broadband access and to analyze new business models. Similarly to what occurs in the energy sector in micro-generation models, in UCNs, the end-user becomes a micro-provider of a specific community by sharing his/her subscribed broadband access within his/her community, as well as by providing specific Internet services, according to specific incentives. Such incentives may simply relate with a well defined human trust (social) network, or even with some form of reward, e.g., gain coverage and Internet access beyond the end-user's premises. They may be user-based; access-provider based; a mix of both cases. Moreover, from a network access provider perspective and at a first glance, the motivation to invest on such models could just seem related

to the possibility to expand capillarity in a low-cost way, as well as to the exploration of new services, which the users can help to define (community-based services). However, UCNs defends that collaboration between access providers and end-users in terms of user-centric networking services opens up new possibilities in terms of business models, based upon a clear separation between the service and network layers, as well as between the network manager and the infrastructure owner. New types of operators that would act as organizers will appear therefore fostering competition and clearly addressing the goal of an open and competitive digital economy.

Technical advantages must be explored from an access perspective and are one of the main aspects to pursue in UCNs. For instance, by deploying UCNs, it is possible to keep traffic local, namely, to take advantage of the physical proximity of sources and destinations and therefore, to prevent traffic from crossing the full access backbone when sources and destinations are "close" (according to previously defined criteria). Traffic locality rules can be applied in a wireless local-loop and will have as consequence a reduction in the access OPEX as well as an optimization of spectrum. Another intuitive advantage is the fact that the subscription relation between the end-user and the access operator can be strengthened by having the access operator empowering the end-user with partial networking functionality, in a way that is completely transparent to the end-user. In other words: such cooperative model (based upon Internet service micro-generation) gives the means for the access operator to provide value-added services that are more appealing to the end-user and that go beyond regular (Triple Play) Internet subscriptions, common today both in the bundled and in Service Provider centric models . For instance, models such as the one embodied today e.g. by FON, when used in strong cooperation with access providers, give the means to access providers to offer Internet access subscriptions with worldwide wireless roaming included, which by itself differentiates such service towards competitors.

This paper contributes to a better understanding of UCNs and their impact in the Internet architectural design and operation. For such purpose, the rest of this document is organized as follows. Section 2 gives insight concerning UCN notions and background, while section 3 covers motivation and details concerning the functional blocks that we believe are essential to consider in any UCN model. Section 4 provides an example of a UCN model that has been conceived and implemented, as well as validated in the context of the European project *ULOOP - User-centric Wireless Local Loop*. The paper concludes in section 5, which also provides pointers for future research in UCNs.

2 UCN Background

UCNs relate to a recent trend in spontaneous wireless deployments where individual users or communities of users share subscribed access in exchange of specific incentives. In addition to the sharing of subscribed access, the Internet user role is augmented in UCNs given that i) the user becomes a producer/provider

of specific services; ii) the user device is part of the network. It should be noticed that this is an aspect that goes against the Internet end-to-end principle, which describes a clear functional splitting between end-systems and the network.Other names in related literature are *personal hotspot*, *spontaneous user-centric networks*.

In UCN, there are two fundamental roles: *node* and *gateway*. A UCN node concerns a role (software functionality) that a wireless capable device takes. Concrete examples of nodes can be specific user equipment, access points, or even some management server. A UCN gateway is a role (software functionality) that reflects an operational behavior making a UCN node capable of acting as a mediator between UCN systems and non-UCN systems – the outside world. The gateway role may or may not be owned and controlled by a UCN user; it may also or only be controlled by an access operator. The key differentiating factor of the role of gateway, in contrast to a regular UCN node, is the operational intelligence and mediation capability. Similarly to UCN nodes, the UCN gateway functionality may reside in the user-equipment, in APs, or even in the access network. Hence, they exhibit a feature that is key in user-centric environments: their behavior as part of the network is expected to be highly variable. Gateways will be active or inactive based on several conditions such as users' wishes and network load.

As previously mentioned, each UCN node has a unique *owner* assigned, which we also name as MP. An owner is an entity (end-user, operator, virtual operator) that is to be made responsible for any actions concerning his/her device. The term "responsible" reflects liability, i.e., from an operator's perspective the owner is the single responsible for the adequate/inadequate usage of the user's device within a specific, trust-bounded community.

A *community* in UCN is a set of UCN nodes that hold common interests (such as sharing connectivity or resources / peripherals) at some instant in time and space. In other words, nodes exhibit a space and time correlation that is the basis to establish a robust connectivity model. This is expected to be extrapolated by adequately modeling trust associations between nodes. We highlight that the notion of community does not have any relation whatsoever to an *Online Social Network (OSN)*, nor even to some specific OSN subset.

An interest is here defined as a parameter capable of providing a measure (cost) of the "attention" of a node towards a specific location in a specific time instant. In other words, an interest is a parameter that provides a node with a measure of a specific time and space correlation. For instance, assuming that a user goes each Saturday morning to the coffee-shop on the neighborhood corner, an interest here could be "having a coffee". Other users in the same location (exhibiting a similar time and space correlation) are in the same place during an overlapping period of time. They all share an interest as they are all collocated in the same location for a specific period of time. The shared interest here is: attending the same coffee-shop. Therefore, owners may be complete strangers and yet, connectivity may be set across the devices, based on parameters such as

specific *Quality of Experience (QoE)* metrics; node movement history; roaming and service sharing patterns.

Fig. 1 illustrates a UCN where two different communities are represented, Community 1 and Community 2. The term community here is simply representative and identifies a set of users within the same WLAN. It could be, for instance, a mesh network in a city, or a hotspot at a coffee-shop.

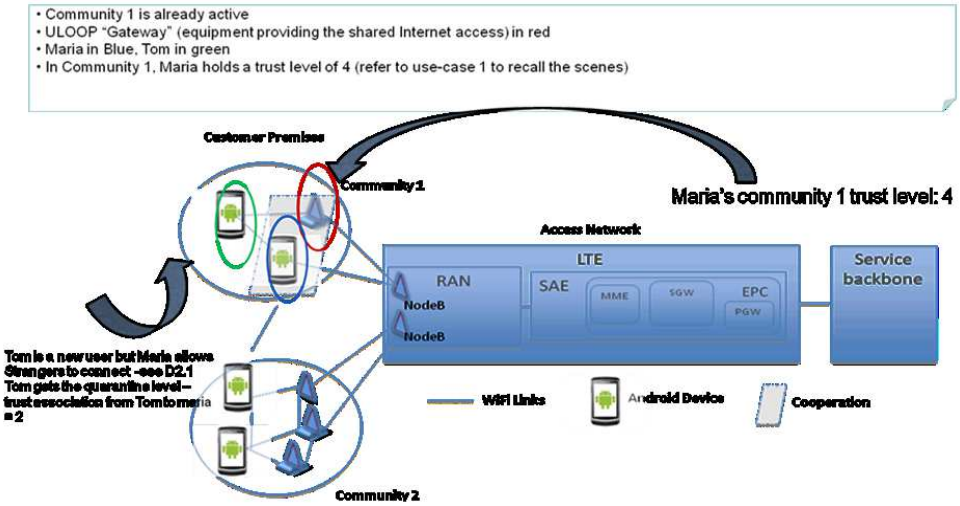

Fig. 1. Expanded capillarity and 3G offloading UCN applicability example..

Community 1 represents an example of a dense wireless network, infrastructure mode (e.g. shopping-mall, football stadium, indoor spaces in a school campus). By dense it is meant that several users may activate devices in AP mode and therefore, there is a strong signal overlap. Hence, the result of this is that despite the fact that spectrum abounds, *Signal to Noise Ratio (SNR)* can be very low in some areas (known as grey areas).

As for Community 2, it stands for a mesh network also interconnected to the same LTE provider. There is no strict relation between a community and a geographic location.

Maria is a user in Community 1 carrying her Android smart-phone (UE). Maria's UE selects a specific gateway (AP or UE) to be associated with in a certain location. After the reception of her association request, the gateway broadcasts a query both via the Wi-Fi interface and the LTE interface (to reach the backend) in order to Fig. out whether Maria is or not an authorized and trusted user. At the same time, the chosen gateway also triggers an adequate gateway selection mechanism that takes into consideration not only Maria's expectations, but also the potential overlap and electromagnetic noise in the area, as well as the optimization of the load across the entire network. While roaming

in Community 1, the gateway onto which Maria's UE is currently associated detects that she is on the move (e.g. due to SNR variations) and immediately attempts to estimate/anticipate a potential new anchor for connectivity (new gateway). Upon agreement between the gateways, Maria's UE is automatically attached to a new gateway which can fullfill Maria's service expectations.

Tom, another user of Community 1, is in a gray area. His device realizes that Maria's device allows connectivity relaying and therefore Tom's device triggers a request to connect to Maria's device. Maria allows other users with whom her device does not yet have a trust association established to interconnect by providing them a small amount of resources based on specific QoE requirements (e.g. only if her UE has enough battery level and up to 20% of Maria's link capacity). Therefore, Maria and Tom's UE automatically negotiate connectivity and Tom goes online through Maria's device. Michael, another Community 1 user, is a subscriber of a network operator different than the one Maria is subscribed to and also belongs to Community 1. Given that they share interests in the context of Community 1, Michael and Maria are able to connect and exchange data directly, without going through their respective operators. Moreover, provided that there is such an available device, Michael can also profit from the Internet access while in Community 1. Every time Michael is within the coverage of Community 1 devices, his UE handovers from the 3G network to community 1 (through Maria's UE). As one of the services provided by the network, all the communication between Michael and other users inside Community 1 is performed locally, including voice and video calls, and thus, for Michael, this means that his traffic is offloaded from the 3G network to the cloud. Whenever Michael leaves community 1 area, his UE handovers back to the 3G network. Thanks to the resource optimization and load-balancing features of gateways within Community 1 continuously exchange data and thus offload / transfer some UE's to other elected gateways. Besides community 1, a second group of users belonging to Community 2 gets information about data being shared in Community 1 (e.g. through the backend system). The second group is located in Paris, at Bob's place. Bob is using a tethered Android powered smart phone to connect to the LTE network and then uses the UCN functionality on the phone, via Wi-Fi, to share Internet access.

A second applicability case is provided in Fig. 2 , where from an end-to-end perspective a single community is illustrated. Community 4 is connected to the Internet by means of a fixed operator (carrier-grade Ethernet/DSL). .

The last hop to the user is Wi-Fi based. We also highlight that the number of UCN communities can profit from services that other users share. In this example the ultimate goal is not to expand coverage but instead to consider ULOOP functionality as an enabling technology platform for cooperative data dissemination. In regular deployments, such data cannot be available, as it is simply the result of a cooperative effort based on a self-organizing system. Moreover, end-user devices that are UCN enabled may be able to gather open data (data collected from the users' surrounding environment). This is, for instance, the case of Maria, who needs to print her boarding pass at an airport with Wi-Fi cover-

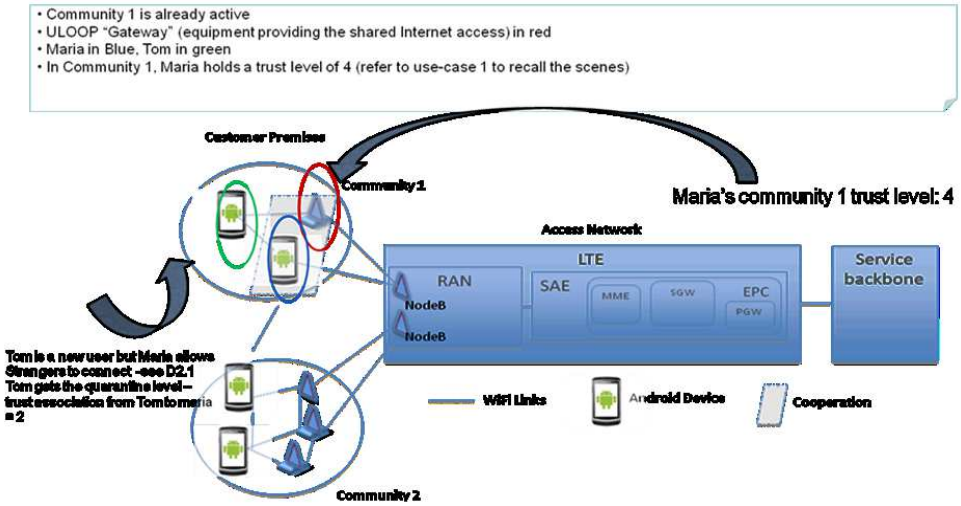

Fig. 2. Traceability and Collective Monitoring UCN Applicability.

age. Due to the UCN functionality implemented in gateways and also provided directly by other users, Maria can print her boarding pass through John's device, a user that Maria's device trusts through a bi-directional trust association.

In Community 4, UCN functionality tracks user expectations and service response. Therefore, users providing expanded coverage have feedback about their resource usage on-the-fly. Moreover, the users are provided with incentives for sharing, e.g. more bandwidth in exchange of receiving some advertisement. Such tracking/monitoring can be performed based on the CPE (UE and gateway) or directly via UE. Moreover, such tracking relates to information that is not personal and that the user always acknowledges to provide beforehand. In this use-case, tracked data does impose neither any confidentiality nor privacy risk for the user. The UE serves the purpose of being part of the data dissemination towards users that share some form of interest, or for which there is some interconnection due to a dynamically established trust circle.

3 UCN Functional Blocks

UCNs envision increasing the potential of the Internet by devising communication and networking technologies which support the creation of techno-social communities, providing a combination of information, communication and human elements, by relying on adequate modeling of trust associations and trust levels. Communication opportunities due to sharing of Internet access as well as due to relaying across multiple hops provide a way to reduce costs, thus creating opportunities for new Internet wholesale models. Hence, new services provided by communities as well as new business models for end-users and access opera-

tors are expected to emerge due to novel features, e.g.an increase in spectrum and energy efficiency in managing wireless communications.

UCNs assume that an existing infrastructure is available and that Internet users are willing to expand such infrastructure in a way that is user-friendly and self-organizing. UCNs assumes also that within specific trust circles some form of cooperation incentives can be provided in order for both the access and the end-user to cooperate and assist in further developing Internet architectures. In order for that to happen, UCNs consider four main functional blocks as illustrated in Fig. 3: trust management and cooperation incentives; resource management; mobility aspects; and backward compatibility.

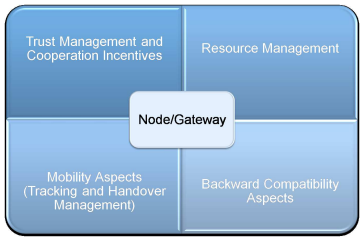

Fig. 3. UCN functional blocks.

3.1 Trust Management and Cooperation Incentives

Trust management and cooperation incentives relates with understanding how to define and build circles of trust on-the-fly. Such circles of trust are capable of sustaining an environment where stakeholders share some form of Internet resources in order to support the dynamic behavior of UCNs. Trust management is based on reputation mechanisms able to identify end-user misbehaviour and to address social aspects, e.g., the different types of levels of trust users may have in different communities (e.g., family, affiliation). In situations where the created network of trust is not enough to allow resources to be shared, devices are able to use a cooperation incentive scheme based on the transfer of credits directly proportional to the amount of shared resources.

Motivating Usage via Cooperation Cooperation incentives in UCN are considered both from a specific technology perspective, as well as from a business perspective. Technical incentives may relate to natural features of the technology that result in a win-win match when cooperation is applied. A concrete example of a technical incentive relates to potential improvements of the 802.11 MAC layer. UCN engineers the MAC layer in a way that mitigates problems related with low data rate stations. Hence, when low data rate stations and high data rate stations cooperate, all elements are expected to take some advantage of

such cooperation. While as for a business incentive, we can think of a specific peering scheme that may assist the access operators in understanding how to obtain revenue based on UCN architectures.

As part of communities and also as individual nodes, cooperation must consider the willingness of owners/nodes in participating in communication. Willingness can be driven by different facts such as energy saving, low processing power, and/or lack of storage room. Although a node is not willing to share resources due to one of the aforementioned facts, the cooperation functionality should encourage such user in doing it so, as he/she can get an immediate return (e.g., more processing) while sharing that resource it has the most (e.g., storage). Instead of simply paying users with the same "currency", e.g., you get more bandwidth if you give more bandwidth, the cooperation functionality should reward involved entities with the type of resource the user wants and at the moment the user needs (i.e., immediately or later on).

The User Perspective The lack of trust between users can influence their level of willingness and our belief is that motivation should be based on shared interests. Users sharing the same interest (e.g., movies), although being completely unknown to one another, can be easily encouraged in carrying information on behalf of others. A user interested in comedy movies surely won't mind to carry a copy of a movie destined to some other user if he/she is able to get a copy also. At this point, cooperation not only helps users disseminate information quickly and seamlessly (as the movie will reach different interested users other than the destination) as it also contributes to sparing resources from users who are not interested in that specific content. Cooperation shall be easily encouraged if users share some social relationship. Thus, social ties have an important role in making cooperation among users even more reliable. Software functionality in UCN nodes is expected to track user expectations and service response. In this case, users are expected to cooperate in order to provide surrounding UCN nodes with information that not only can improve their own but also the other users' network experience. Users can exchange: i) SNR information, e.g., to aid in the handover process; ii) behavior information, to strictly penalize malicious/greedy users; iii) connectivity quality levels, to aid in load balancing and interference reduction.

The Provider Perspective UCN is a perfect solution for operators who are looking for higher density at limited cost, letting them to rely on created communities, in order to provide the required resources to demanding users at specific instants in time. This will offer an energy-efficient and cost optimized solution to increase density of the operators' networks. Moreover, the subscription relation between the end-user and the access operator can be strengthened by having the access operator empowering the end-user with partial networking functionality, in a way that is completely transparent to the end-user. In other words: such cooperative model (based upon Internet service micro-generation) gives the means for the access operator to provide value-added services that are more appealing

to the end-user and that go beyond regular subscriptions, common today both in the bundled and in Service Provider centric models such as the one embodied today by e.g. FON, when used in strong cooperation with access providers, give the means to access providers to offer Internet access. For instance, access operators can take advantage of UCN capabilities to further expand its control towards the customer premises devices.

Some reasons for UCN adoption (and hence for the relevancy of operator-based incentives) are: to provide adequate feedback to customers; to ensure an optimal network operation, where expanded coverage is also offered; to be able to deal with interference in dense areas; to provide residential areas with the same authentication/authorization model used in UCN coverage and thus, reduce CAPEX; to gain in reputation by supporting communities, following what is today common practice in open-source business models.

An "Open Source" model with "some limitation" can favorite a win-win equilibrium between UCN and operator's competitiveness goals. Hence, operator's based incentives are expected to improve the potential of interoperability and of business opportunity for access and service stakeholders.

3.2 Augmented Resource Management

As UCN relies on wireless infrastructures that are often deployed in an ad-hoc way, resource management optimization is a key aspect to pursuit. UCN has as purpose to assist in developing robust and high debit wireless local-loops in a way that meets current broadband access technologies debit as possible, and in a way that reduces the chances for bottlenecks to occur. Throughput maximization is to be addressed across more than one hop by means of cooperative networking techniques of which one possibility is relaying. In regards to resource management, and to achieve a fair and self-organizing network operation, there are aspects to be looked for such as the need to adequately and dynamically be able to control growth of UCN communities; dynamic fluctuations of the network both in terms of traffic due to stations joining and leaving frequently, as well as due to the movement of stations. Another aspect that is considered crucial to look for is to develop cooperative and distributed mechanisms that assist the network in adequately selecting nodes that are willing to be micro-providers. Such selection is to be performed in a way that considers not only throughput maximization, but also the lowest-cost in terms of energy-efficiency.

3.3 Dealing with Frequent Roaming: Anchor Point Control and Movement Estimation

UCNs are based on the notion of users carrying (or owning) low-cost and limited capacity portable devices which are cooperative in nature and which extend the network in a user-centric way, not necessarily implying the support for networking services such as multi-hop routing. For instance, in UCNs transmission may simply be relayed based on simple mechanisms already existing in end-user devices. These emerging architectures therefore represent networks where the

nodes that integrate the network are in fact end-user devices which may have additional storage capability and which may or may not sustain networking services. Such nodes, being carried by end-users exhibit a highly dynamic behavior. Nodes move frequently following social patterns and based on their carriers interests; inter-contact exchange is the basis for the definition of connectivity models as well as data transmission. The network is also expected to frequently change (and even to experience frequent partitions) due to the fact that such nodes, being portable, are limited in terms of energy resources.

In terms of mobility and adding to the currently available solutions, UCN is focused on two main aspects: mobility tracking and estimation, as well as handover support. Ways of addressing patterns of node movement to estimate mobility patterns based on existing or novel social models is one aspect to be addressed [12]. The purpose is to assist in improving the underlying connectivity model, and hence overall network operation. Social mobility modeling is an aspect that assists in deriving algorithms and functionality that can anticipate the way nodes move based on analysis and tracking of node movement through time.

A final aspect to consider is to ensure that the functionality to be developed can assist in dealing with the unmanaged aspects of UCN architecture and should get rid of anchors in the network. This may be required, for instance, if a UCN community is not capable of providing a node with adequate mobility management e.g. due to trust aspects.

Being focused in Wi-Fi, the regular 250 meters range is small compared to the geographic distances that users are expected to travel in UCN scenarios. Hence, performing a complete handover would impose strong requirements on speed of message exchange. In UCN this is to be tackled by considering the regularity (routine) present in users' movement, which may assist in determining the place and type of resources that may be required to set up to assist seamless handovers. For example, based on movement analysis, the system may determine with a high probability that the user will handover towards the range of UCN gateway A or UCN gateway B. In this case specific functions may assist in defining the adequate next target, and how to handover to it. The challenge here is to identify with enough accuracy and reliability the gateways that a UCN node should connect to, while moving.

3.4 Backward Compatibility

When dealing with unaware systems, i.e. systems that do not support UCN functionality, it is important to consider that a UCN device needs to be available to connect to a "legacy" network, and therefore, we must ensure proper backward-compatibility. This implies handing the interoperability aspects that deal with existing networking models and paradigms. Interoperability with legacy networks is especially important in the case where nodes roam through different types of networks, such as mobility between UCN and other types of networking architectures. Interoperability also relates to backward-compatibility, i.e., assisting

devices outside of UCN to be able to participate in UCN communities in a regular way. Regardless of who supports the community information for the agnostic nodes, the connection, access must remain transparent (limitations can apply). Therefore, by allowing legacy nodes to connect to a UCN supported community, the trust and resource management implications must be considered. Within these aspects, the solution greatly depends on how much interoperability is required, and at which phase should it be considered (either as design constraint or proxy/adaptation/add-on functionality). The impact on different functionality can be substantial, depending on the type of integration/interoperability required.

4 An Architectural UCN Model: the ULOOP Example

In this section we provide a model for UCN that has been conceived, validated, as well as implemented in the context of the European project ULOOP, being currently available to the community as open-source LGPLv3.0 software [3,2].

ULOOP considers a software-defined approach to implement the UCN architecture, based on a modular approach. A unique software suite is provided to devices, which then take the role of node or gateway, depending on a series of external conditions. The next sections provide input into the ULOOP architecture, which is composed of three main entities: the Trust Manager entity; the Resource Manager entity; the Mobility Aspects Entity. Each of this entities comprises specific sub-modules that are dynamically activated depending on the role assumed by a device implementing ULOOP.

4.1 The Trust Manager Entity

In ULOOP, trust management and incentives for cooperation are related to understanding how to define and build circles of trust on-the-fly to provide the user with liability[14]. Trust management is based on reputation mechanisms able to identify end-user misbehavior and to address social aspects, e.g., the different types of levels of trust users may have in different communities (e.g., family, affiliation). In situations where the created network of trust is not enough to allow resources to be shared, ULOOP devices are able to use a cooperation incentive scheme based on the transfer of credits directly proportional to the amount of shared resources [4,6,13]. Trust Management here is split as follows: i) Identity management; ii) trust setup; ii) trust management iii) cooperation and rewarding.

Trust Setup Trust setup in ULOOP is a one-time process that a user (owner) executes on one of its devices. This process does not need to be repeated on other devices of the user. After the setup procedure, the trust value may be updated based on a new value for the dispositional trust value, which can be always adjusted in each of the devices owned by the same user as a first step. It is worth mentioning that the trust setup process may be repeated; a user is

always free to request a new crypto-id and nickname for each of his/her devices (by ticking the option "yes" when the ULOOP setup asks if this is the first device ever in ULOOP for that given user). Trust setup is triggered in any ULOOP node and comprises a series of steps which result in: i) a unique identifier, the crypto-id; ii) a wallet with an initial set of credits; ii) an initial trust value towards any new neighbor, familiar or not – dispositional trust.

The first step towards building trust references in communities, i.e., from a ULOOP node to others, is to be able to uniquely identify owners of ULOOP nodes. Ideally, the recognition must be attack-proof. Hence, the end-user must be able to authenticate her/him. However, it also important to protect the privacy of this end-user, so this building block contains both identity management and *Privacy-Enhancing Technologies (PETs)*.

ULOOP reuses the concept of crypto-identifiers (*crypto-ids*) based on asymmetric cryptography. With such crypto-ids, the end-users can prove in a decentralized way and with cryptographic strength that they really own the secret linked to the crypto-id. Concerning privacy, creation and proof of ownership of crypto-ids does not require a centralized identity authority. Thus, end-users in ULOOP will protect their privacy through crypto-ids that they generate themselves and act as their pseudonyms not linked to their real world identity. The crypto-ids are based on a set of information provided to the user by an authorized entity (e.g. the personal identification number embedded in a citizen identity card provided by a government to any citizen, or a mobile phone number associated to a unique SIM card). Such personal identification number will be used to generate a unique crypto-id based on a hash function that is implemented in any ULOOP node or gateway. The local generated crypto-id will need to be verified by an authorized entity in order to allow the ULOOP node/gateway to gain full access to the ULOOP community.

When such verification cannot happen, the ULOOP device gets a minimum trust level in the community, allowing it to use a predefined set of minimum resources.

In ULOOP, owners are likely to be responsible for more than one active device. One would be a primary device, and the remainder equipment will share the same crypto-id generated by the first personal device, as well as the reputation level and trust associations associated to the unique crypto-id. This is possible by using secure in range wireless or wired communications. Synchronizing the reputation levels and trust associations among personal devices will allow the user to always make use of the earned reputation level, trust associations and credits that resulted from the usage of the unique crypto-id in another personal device. Synchronization of trust information can be done by using prior-art on file and data synchronization. The validation of the unique crypto-id can be done by making use of any opportunity to access the Internet (limited Internet access should be allowed by the minimum trust level). This may create some problem in extreme cases, in which Internet access is not possible for a long time. However, such scenarios are more related to delay-tolerant networks and not to ULOOP, in which it is expected that trust management and cooperation incentives will

create the conditions to make Internet access more pervasive than today. Nevertheless, it is clear that the usage of a unique crypto-id may limit the usage of ULOOP in fully decentralized environments, namely in the presence of isolated ULOOP networks (without any Internet access whatsoever) and new users (that still need their crypto-ids to be validated).

UCNs such as ULOOP are supported both by static, fully dedicated nodes as well as by nodes provided by end-users on-the-fly. Since some nodes are carried by Internet end-users, their networking composition, surrounding environment and organization can rapidly change. As such, the dispositional trust level on a given node might not be appropriate in all circumstances and should be able to be adapted and changed over time, in order to protect the node's integrity. The process of dispositional trust adaptation might occur in two different cases: i) the node has a dispositional trust level that is inappropriate and leaves it too open to attacks; ii) The node joins a different community than the initial one in which the dispositional trust level had been setup.

An untrustworthy node in ULOOP goes through a boot-up procedure where the node may be the first one an owner is responsible for, or one of several nodes. In the former case the owner is prompted to set its *Dispositional Trust (DT)* level [16], e.g. being able to select from a list of predefined values, which range from 0 to 100, being 0 "paranoid" which means that a priori the node will not trust anyone, and being 100 "blind trust" which means that the node will trust no matter what. In the second case, the user is presented with two options: i) to clone the dispositional trust level assigned to other devices that are already in ULOOP and that she/he owns, for the usage of unique crypto-ids in different personal devices: ii) to assign a new DT level for the node being introduced, as explained in the previous paragraph.

After the one-time step of trust setup, any node starts in background a trust management process.

Trust Management Trust management is performed in two different phases of ULOOP: i) when connectivity is attempted; ii) during data transmission. When a node attempts to connect to a wireless network (e.g. via a captive portal), this triggers a request for resources, an aspect that is tackled by the Trust Manager entity in ULOOP.

The Trust Manager entity is in charge of executing the main, and establishing and maintaining the external interfaces (communication via TCP sockets, for the sake of proof-of-concept) with the Trust Manager of other ULOOP nodes (requester to requestee and vice-versa), as well as the internal interfaces with other operational modules (Resource Manager and Mobiliyu Aspects) within the same node. When first instantiated, the Trust Manager performs a series of initial setup procedures, such as the virtual crypto-id generation and validation, as well as the dispositional trust setup. After this, and before going to the main operational mode, it starts a set of periodic activities from the reward manager that have to be executed in the background in order to ensure the proper operation and update of the bank account and the wallet of the node. Finally,

the main functionality allows the node to perform its main operation, such as exchanging crypto-ids with other ULOOP nodes in order to start a cooperation process, performing social trust computation of those nodes and carrying out the control of cooperation, fundamental to decide if a service is obtained or allowed from/to another node.

Cooperation and Rewarding The computation of trust is provided by a dynamic cost function, implemented via the sub-module social trust computation. Then, ULOOP contains an entity, the *Cooperation Manager (CM)*, that is responsible for coordinating the cooperation. On the control of cooperation, if the device is a requester and requires a service, it must compute the amount of credits that will convince the prospective requestee in engaging in cooperation. Then, a Reward Manager entity takes care of controlling promises of payments, and payments itself, in coordination with the Cooperation Manager entity.

At bootstrap, the Cooperation Manager entity starts by assigning an initial amount of cooperation credits to the user. This initial amount takes into consideration the node trust level and established minimum and maximum amount of credits thresholds for ULOOP devices. As the Reward Manager handles credits, the Cooperation Manager informs it of this amount in order to make the Reward Manager aware of how much cooperation credits the device has. During negotiation, credits are used by the requestee to express the cost of the service/resource he/she provides. The negotiation phase is positively concluded if and only if an agreement is reached both in terms of service level and in terms of credits between requester and requestee. In ULOOP trust can also be used as a parameter to affect the cost of the negotiated service. The ULOOP incentive framework is open to the implementation of any functional relation between cost and trust.

On the control of cooperation, if the device is a requester and requires a service, it must compute the amount of credits that will convince the prospective requestee in engaging in cooperation [18]. Additionally, as the tokens are the common language among the different managers, a number of tokens is computed by means of Social Trust Computation and a promise of payment is done by means of Reward Manager. Then, the CM sends (by means of external interface made available to all modules of the Trust Manager) a service request to the potential requestee, which in turn replies specifying whether or not it will engage in cooperation. In the case the device is a requestee, it receives the service request and evaluates whether the received credits are enough to provide the requested service. Then, a check on the amount of resources is done is order to assess whether the requestee can answer the service request. If so, the requestee (i.e., Reward Manager) accepts the received amount of credits, Social trust Computation updates the trust level, and issues a service reply informing the Cooperation and Trust Managers that requestee is ready to engage in cooperation.

The CM is expected to run in the both ULOOP node and gateway. The role of a device will be set by detecting the conditions around and feeding that data to the respective daemon. For instance, a device may become a gateway because

it is connected to the Internet and if it has the required trust level. So, if by some reason the trust level changes, that node may be automatically prevented from becoming a gateway.

The Reward Manager is the ULOOP software module that handles payments and credit transfers, used as additional rewarding incentives for cooperation. Credit transfers revolve around credit units, which are a form of virtual currency. The Reward Manager software module has been characterized in a way to ensure that the transmission of credits is validated and secure, by preventing the creation of fake credits and the forging or duplicating of payments. The resulting virtual currency model is secure and, while being centralized in nature, allows the nodes to exchange credits when offline. The Reward Manager is a software module running in each ULOOP node. The module does not require any additional external interfaces and it provides a set of APIs (in the form of function calls) that can be directly used by any other ULOOP module on the same node. Communication between nodes and the central authority managing credit exchanges and ownership (also known as the "Bank") requires HTTP connectivity. Software in need of exchanging credits must use the Reward Manager's APIs. The system allows users, uniquely identified and registered with the central authority (Bank), to generate credits when registering into the system for the first time and to exchange such credits between registered users at any time. Each payment is uniquely identified. Payments may be made and exchanged even while disconnected from the Internet, but they must eventually be acknowledged by the Bank in order to be processed. The Reward Manager is expected to run in both a ULOOP node (end-user equipment) and on a ULOOP gateway (e.g. Access Point).

Social Trust Computation The computation of trust is provided by a function implemented in ULOOP nodes and gateways. Trust computation is a dynamic cost function that has to be sufficiently strong to provide, based on a local perspective, attack resistance. It comprises therefore the dispositional trust of a node, as well as evidence concerning contacts with other nodes. To explain the notions behind social trust computation we provide an example based on three nodes: node A, the node that is about to compute a trust level towards a node B, and node C representing a node in the same community as node A. Node A has a dispositional trust level e.g. 0.5. In order for node A to compute the trust association cost towards node B, it takes into consideration recommendations sent by nodes belonging to the community. Such recommendation may be direct, i.e.,the node has a direct trust association to node B, or indirect, i.e., a node has an indirect trust association to node B with the association being established through some other node, e.g., C.

Direct trust associations are more relevant (have more weight on the trust cost function) than indirect recommendations. Recommendations provide with a trust cost that nodes in the community have towards a new node. A direct recommendation received by node represents an answer from a node in the community, and contains the computed cost of one or several trust associations between and

the target node. An indirect recommendation received by a node represents an answer from a node in the community which contains the computed cost of one or several trust associations between and the target node, but is not yet in the trust table of that node. ULOOP proposes a specific trust computation function which considers both direct and indirect recommendation values, as well as the owner's own beliefs - dispositional trust. Moreover, the more stable acquaintances are, the more trusted their recommendations become. Other functions may be applied easily via the interfaces created for such purpose.

The operational behavior of this module is as follows. After boot up the nodes check for their dispositional trust D and activate a trust table. The trust table is a structure where each row is a tuple with the following structure: $<$*Node Id, trust level, aging*$>$. When activated, the node provides each of its neighbors with an equal trust level of D. In other words, in environments where relations were not yet established, ULOOP nodes trust equally all nodes around. Then, the trust table can be periodically updated via recommendations by neighbors to assist in computing periodically the trust table of each node. Requests for social trust computation come from the trust manager, cooperation manager and are provided via a look up to the trust table.

4.2 The Resource Management Entity

In ULOOP the management of network resources takes advantage of the willingness that users have in cooperating, based on the mentioned two types of incentives: trust-based and reward-based.

The resource management operation takes place for nodes that have credits and are trusted in the community. The resource management operation itself starts when a Gateway gets a request for resources. This request is mainly from trust management block on a ULOOP gateway. If the resources are available in the Gateway, the resource management block provides a positive feedback to trust management and the new node can then join the network. The resource management block also provides updates about the channel to the mobility aspects functional block.

4.3 Call Admission Control based on Trust

Call Admission Control (CAC) is responsible for checking if there are available resources, on the gateway, to accept or deny a request from RM. The CAC is only enabled on the requestee side (gateway). After the RM initializes the CAC function, the CAC stays in an idle state until a RM calls CAC or when the thread, scheduled to run before, wakes up to check the priority queue (pqueue). When the RM calls CAC, CAC handles the incoming request, prioritizes it, and puts it on a virtual queue, *pqueue*. After this, CAC schedules the thread to run. When the thread wakes up, it checks if the pqueue is empty or not. If not, it enqueues the request with highest priority and then checks if the gateway can accept it or not. Acceptance is provided by another sub-module, responsible for resource allocation, the *Elastic Spectrum Management (ESM)* functional block.

Resource Allocation ULOOP is envisioned to be applicable to dense area networks, which face, among other problems, the issue of interference. Moreover, in these environments, spectrum abounds and is underused. In ULOOP and in addition to augmented call admission control and self-organizing mechanisms to elect and to select gateways, a key aspect to be developed relates to considering mechanisms that allow the MAC layer to become more elastic in multi-user environments in a way that is fully backward compatible with current IEEE 802.11 standards. This is achieved by just working with the current MAC frame format, and with the interpretation of such frames by ULOOP nodes [21].

Resource allocation in ULOOP follows the recent trend concerning frequency assignment and sub-division which argues that the channel width of nodes should be adaptive, in particular by considering an alternative way of arranging wireless channel assignments, based on *Orthogonal Frequency Division Multiplexing (OFDM)* . OFDM is supported by IEEE 802.11a/g/n standards, which are the ones that are dealt with in ULOOP. To achieve this purpose - which ULOOP named *Elastic Spectrum Management* (ESM) - resource allocation integrates a new mechanism that employs adaptive multi-user access, modulation, error coding and power allocation techniques to judge the tradeoff between costs vs. performance gain [5,9,8].

ESM is initialized by the RM, indicating which mode the ESM must work, as a gateway or as a station. For the gateway mode, the ESM is responsible to assign a number of bits to a station depending on the number of tokens. Each station connected to the gateway has its own number of bits. This number will be used to create a super-frame, containing multiple parts of different payloads of each station. A station with a higher number of tokens, compared to the others stations, has the right to write more data inside the super-frame. A station with the least tokens may get to write less data or even nothing inside the payload, in case the 6 slots, each corresponding to 8 bits, have already been assigned to others stations with higher number of tokens. After the slots have all been assigned to the stations, the ESM will create the super-frame and send it to the driver for transmission.

Still in the context of resource allocation ULOOP researched cooperative diversity techniques at the MAC Layer, mechanism entitled RelaySpot [22,10,11]. Cooperative relaying is quite helpful in IEEE 802.11 networks, since terminals end-up with different data rates due to the rate adaptation mechanism. Terminals far away from an AP may grape the medium for long time to complete their slow transmission. Relaying data over a node that has better data rate towards source and AP will release the medium earlier and providing better throughput and reduced delay.

Cooperative Load-Balancing Due to the dynamic behavior of ULOOP, nodes willing to share resources are more prone to be exposed to interference due to associations of other nodes. One of the aspects that is required to consider based on a self-organizing behavior that is inherent to ULOOP gateways is to assist in preventing excessive resource consumption, i.e., by performing network load

optimization [7]. Part of this mechanism relates to being able to shift in an optimal way stations across different gateways and also to be able to adequately perform load-balancing among gateways. The aggregation of resource utilization, QoS and QoE measurements in a semantic form is the reasoning mechanism of the decision-making engines having the responsibility of load balancing trigger. Resource consumption monitoring that works in a passive way provides ULOOP gateways with the ability of classifying its clients according to bandwidth usage. The gateway arranges the client Id's with respect to their bandwidth consumption and marks the most consuming stations as "resource hungry". With this categorization, gateways can be aware of nodes that are less beneficial to the system, and if required assist their handover to other gateways while balancing load in the network in a fairer way.

4.4 The Mobility Aspects Entity

From a mobility perspective UCNs exhibit a highly dynamic behavior where the selection of the "best" mobility anchor points requires the pursuit of two main aspects: adequate selection and redundancy. This has to be achieved by always weighting user expectations and the support each user is willing to give as well as the network support (access sharing) each user can in fact provide to its counterpeers in the network. Mobility anchor point location and selection optimization is therefore a crucial requirement of UCNs. Mobility anchor points may be part of the SP equipment, of the NAP equipment (edge node) or in fact be part of the equipment of the MP and this can increase heavily a UCN complexity.

Achieving a Better Control of Mobility Anchor Points The *Mobility Anchor Point (MAP)* is developed in ULOOP to be extended and adapted in the mobility anchor function of an existing mobility management solution. It interacts with resource management to get the resource information in the gateway and registers its context and sends keep alive message to the *Mobility Coordination Function (MCF)*. This sub-module takes care of coordinating the selection of MAPs based on resources; trust aspects; QoE. Based on the number of currently known active MAPs it is responsible to perform a MAP selection decision for the ULOOP node upon receiving MAP request from the MAG, which are then enforced on the data path.

Estimating Node Movement ULOOP has addressed how to assist the network and the user in terms of mobility, by allowing devices to infer future roaming behavior, based on a selection optimization that simply relies on data available to devices, and which concerns visited networks [20]. Concrete examples of network parameters include, but are not limited to: number of visits performed over a specific period of time, e.g. 24h; average duration of one visit; visited network attractiveness, e.g. trust level that a node has towards a specific gateway that is regularly visited; number of visits accepted/authorized; time elapsed since the last visit to a specific visited network.

For each visited network, nodes compute locally, seamlessly, and periodically a cost (a ranking parameter) based on a specific formula that relies on the collected network parameters. That ranking parameter is also stored in the listing of visited networks. As proof of concept, ULOOP has worked these concepts and integrated them into the end-user background application MTracker (Mobility Tracker), currently available to be applied in the majority of portable devices, Android included. Based on data available and passively collected, the MTracker application then tries to predict in how much time the node will change the network connection, and which will be the next network, passing this information to the server side, e.g. to the MCF, which then decides how to handle such information.

5 Summary and Conclusions

UCN envisions increasing the potential of future Internet architectures by devising communication and networking technologies, which support the creation of techno-social communities. For such purpose UCN considers knowledge derived not only from networking paradigms, but also from social trust modeling as well as by taking advantage of an adequate estimation of potential communication opportunities (e.g. sharing of Internet access and relaying resources) even if devices belong to users that are not socially acquainted. The expectations concerning UCNs are, from a business perspective, the opportunity to develop new community services and hence to derive new business models for Internet stakeholders. From a technical perspective, software defined ways to improve the network operation e.g. in regards to spectrum usage or energy-efficiency.

The paper provides notions concerning UCNs as well as describes an implementation for the ULOOP software architecture, representing an instantiation of UCNs which is currently available to the community.

Relevant research opportunities in the context of UCNs are related with the application of trust as a potential parameter that stemming from social sciences can be applied to Quality of Service as a way to create more robust Internet architectures. Another relevant field to be addressed is direct trading of resources on the network, as a way to develop new business models.

References

1. R. Sofia and P. Mendes. "User-provided Networks: Consumer as Provider", IEEE Communication Magazines, Feature Topic on Consumer Communications and Networking - Gaming and Entertainment.Volume: 46 Issue: 12 Pages: 86-91, December, 2008.
2. Paulo Mendes (Editor). "D3.8: ULOOP Framework Specification and validation, October 2013. ULOOP European project deliverable (gr. Nr 257418) .
3. Alfredo Matos (Editor). "D3.9: ULOOP Software Suite". October 2013. ULOOP European project deliverable (gr. Nr 257418).
4. A. Aldini, A. Bogliolo. Model Checking of Trust-Based User-Centric Cooperative Networks. W-PIN2012, April 2012.
5. H. Haci. Novel Scheduling for a Mixture of Real-time and Non-real-time Traffic. IEEE GLobecom 2012, Best paper award. September 2012.
6. A. Aldini, Trading Cooperation Incentives and Performance in UCNs. Quasa ES-ORICS 2012. July 2012.
7. M. Yildiz. Cooperation Incentives Based Load Balancing in UCN: A Probabilistic Approach. IEEE Globecom 2012. July 2012.
8. H. Zhu and J. Wang, "Chunk-based resource allocation in OFDMA systems - part I: chunk allocation," Communications, IEEE Transactions on, vol. 57, no. 9, pp. 2734-2744, 2009.
9. H. Haci, H. Zhu and J. Wang, "Resource Allocation in User-Centric Wireless Networks", VTC-Spring, 2012.
10. T. Jamal, Paulo Mendes, André Zuquete, "RelaySpot: A Framework for Opportunistic Cooperative Relaying", ACCESS conference, Luxembourg, June 19-24, 2011.
11. T. Jamal, Paulo Mendes, André Zúquete "Interference-Aware Opportunistic Relay Selection", in Proc. of ACM CoNext (student workshop), Tokyo, Japan, December 2011.
12. Andréa Ribeiro, Rute C. Sofia and André Zúquete, Improving Mobile Networks based on Social Mobility modeling, IEEE International Conference on Network Protocols, 2011.
13. Alessadro Bogliolo, Saverio Delpriori, Lorenz Klopfenstein, Alessandro Aldini, Jean-Marc Seigneur and Waldir Moreira Junior, Crediting Aspects in ULOOP, ULOOP White Paper 09, 2012.
14. Carlos Ballester, Jean-Marc Seigneur, Paolo di Francesco, Valentin Moreno, Rute C. Sofia, Alessadro Bogliolo, Nuno martins and Waldir Moreira Junior, A User-centric Approach to Trust Management in Wi-Fi Networks, IEEE INFOCOM - Demos Track, 2013.
15. H. Haci, H. Zhu, J. Wang . Resource allocation in user-centric networks. VTC2012, May 2012.
16. C. Ballester, Jean-Marc Seigneur. Dispositional Trust Self-Adaptation in User-Centric Networks. In Proc. of AINA, March 2013.
17. A. Aldini. Formal Approach to Design and Automatic Verification of Cooperation-Based Networks. IARIA International Journal On Advances in Internet Technology, June 2013.
18. A. Aldini. A. Bogliolo. Modeling and Verification of Cooperation Incentive Mechanisms in User-Centric Wireless Communications. Book chapter in Danda B. Rawat, Bhed B. Bista and Gongjun Yan (Editors), "Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications" IGI Global, 2013.

19. EU IST FP7 ULOOP - User-centric Wireless Local Loop project, 2010-2013, grant number 257418. Available at http://uloop.eu/.
20. R. Sofia. "Method and Apparatus for Ranking Visited Networks" (EP 13186562.9). August 2013.
21. H. Osman, H. Zhu, H. Haci, L. Lopes, R. Sofia. "Method and Apparatus for communication in a wireless network" (EP 13191667.8), August 2013.
22. T. Jamal, P. Mendes. "Cooperative Relaying for Dynamic Networks" (EP13182366.8). August 2013.