Trust as a Fairness Parameter for Quality of Experience in Wireless networks

Rute Sofia*, Luis Amaral Lopes

COPELABS, University Lusófona, Lisbon, Portugal
{rute.sofia,luis.amaral}@ulusofona.pt

Abstract. This paper addresses the applicability of trust metrics as a fairness parameter in call admission control within the context of user-centric networks. The paper explains how trust can assist in improving user Quality of Experience in wireless networks, by taking into consideration not only channel conditions, but also trust levels derived from the interaction that users have in the context of Internet shared services.

1 Introduction

Wireless revolutionizes local area communications allowing citizens to provide communication services as well as to become micro-providers in *User-centric Networks (UCNs)*. This emerging networking paradigm relies in the user's willingness to share connectivity and resources. In comparison to traditional Internet routing scenarios (be it based on wireless or fix line technologies), UCNs bring in forwarding challenges, due to their underlying assumptions, namely: i) end-user device nodes may behave as networking nodes, ii) nodes have a highly nomadic behavior, iii) data is exchanged based on individual user interests and expectations.

Furthermore, emerging trends such as UCNs adding to the development of faster, more reliable wireless standards, miniaturization of devices, and reduced costs of hardware and services, is leading to a fast evolution of technological as well as societal aspects in the way that people communicate. For instance, people expect to be able to send and retrieve information whenever and wherever they want. Yet, there are technological limitations which may affect this anytime-anywhere communication paradigm, e.g. gray areas (i.e., areas where the wireless signal strength is not enough to sustain connectivity); physical obstructions; limited battery devices; environmental aspects; limited resources and security issues. Related literature has been addressing aspects to mitigate wireless interference and to take advantage of cooperative diversity which may mitigate some of the problems posed by physical obstructions and coverage problems due to node mobility. However, it is imperative to say that, since information is relayed among nodes and these nodes can be highly dynamic, communication

* Corresponding author. COPELABS, University Lusófona, Building U First Floor, Campo Grande 388, 1749-024 Lisbon, Portugal.

may experience delay, varying from short to long periods, as isolated areas (e.g., intermittent connected networks) may form in the case of node failure (e.g., damaged *Access Points, APs*) or mobility (e.g., user changes position). Thus, to increase the performance of multi-hop communication, several improvements can be made, by taking advantage of transmission opportunities provided by moving nodes and accessible APs, for instance. An example for such an occurrence is a citizen at a public location without Internet access. If Internet users are in the vicinity, and such users are part of a UCN, then some of them may share Internet access and data can be relayed until it reaches the closest Internet gateway. Another situation may occur when information is simply carried by users that happen to be moving towards the place where the destination is located. Nowadays, this is possible thanks to the size of devices which are making them easier to carry around, and also to the resource capabilities they have. For instance, the HAGGLE EU project [1] exploits store-carry-and-forward capabilities (i.e., devices' powerful features, user willingness, trust among users, opportunistic contacts) aiming to provide communication in scenarios with intermittent connectivity. HAGGLE considered human mobility and the power of users' devices to perform forwarding of information independently of the network layer. So it is easy to see that the way people communicate is arriving at a point where such communication must happen independently of the infrastructure available, and depending on the capabilities of intermediary devices as well as their mobility pattern, interests and social ties.

In what concerns the network layers, this new communication paradigm demands more reliable and efficient protocols, as today we have areas where spectrum abounds and creates interference - dense networks, e.g. residential households, shopping malls) as well as areas where communication is only possible through the formation of clusters of users (e.g., intermittently connected networks). Even in a metropolitan area, intermittent connected networks exist due to wireless environments, unexpected disruptions, and areas where the networking infrastructure is sparse (e.g., city parks).

A key factor that has assisted so far the expansion of UCNs in an indirect way, is trust as perceived by humans in social networking. Living examples of UCNs have expanded solely by the willingness of the end-user to become part of these communities, i.e., to *trust* unknown users and to allow others to rely on privately owned APs. Hence, these networks and their scalability is basically growing due to the Internet end-user's belief that the benefit of relying on UCNs is higher than the risk, which in itself is a pure social belief that can be applied in networking to improve the network operation [14].

UCNs integrate the notion of social trust schemes thus allowing users and operators to develop connectivity between devices based on trust circles. Such trust does not necessarily imply that users know each other; instead, it relates to *social interaction* and to the interests shared by familiar strangers, i.e., users that knowingly or unknowingly share some aspects of their daily routines (e.g. visiting the same coffee shop every Saturday morning). Hence, the user anonymity is kept, while social interaction metrics related to direct and non direct recom-

mendations of nodes around, as well as to the trust openness of a user towards strangers assists in developing more robust connectivity links, in the sense that connectivity becomes intertwined with circles of trust that are built on-the-fly.

In addition to assist in creating, under specific circumstances robust connectivity on-the-fly, trust is also a *Quality of Experience (QoE)* parameter which can be applied in networking to improve the satisfaction of users involved in UCNs, and hence contribute to a better, in the sense of fairer, network usage.

This paper explains such notions, namely, how can trust, a social parameter based on individual beliefs, be applied in the context of resource management in wireless networks, in particular in environments such as UCNs where the end-user is a stakeholder of Internet connectivity. The paper is organized as follows. Section 2 describes work that shares our motivation. Section 3.1 goes over the trust application in the context of QoE and network fairness, while section 4 gives insight into how trust can be applied to *Call Admission Control (CAC)* in the context of wireless networks, based on a specific proof-of-concept that has been developed for UCNs. The paper concludes in section 5, providing a few guidelines for related research.

2 Related Work

Resource management in wireless networks and in particular call admission control is a topic that has been central to *Quality of Service (QoS)* research in wireless networks, for the last decade. Several schemes have considered ways to ensure fairness, being usually the intention to allow the network to serve more users at an instant in time [3]. Initial approaches considered static or dynamic threshold models [5] and priorities to provide fairness in terms of network utility, e.g. throughput. Pong et al. provided an analysis of the trade-off between fairness and capacity in the context of *Wireless Local Area Networks (WLANs)*, for scenarios with interference. This work explores fairness in terms of throughput as a measure of network utility, and allowed transmission time, explaining how different fairness parameters impact on the capacity of the link. Pricing model approaches [6,11] were applied to ensure fairness, again in terms of network utility, but considering all of the potential network stakeholders. Game theory has also been considered as a way to assist a better notion of fairness in wireless networks [10].

More recently and due to the user-centric networking trend in wireless networks, the need to consider *Quality of Experience (QoE)* metrics that could assist a more dynamic behavior where the network can serve better more users as well as to increase user satisfaction emerged. Neely provides QoE networking contextualization in terms of QoS, for which parameters are more easily understandable, from a networking perspective [9]. Piamrat et al. consider mean opinion score (MOS) without interaction from real humans [7] and provide a simulation based performance evaluation showing that not only was the network better used in terms of throughput, but user satisfaction was also increased. Still in the context of translation between QoE and QoS, Zhang et al. explains the

challenges and a possible solution to optimize QoE in next generation networks [12].

Our work builds on the need to integrate QoE, namely, the intention to allow more fairness in the way users are served by the network, while at the same time achieving better network usage. To achieve this we follow a dynamic approach, by considering the trust level that users have on thirds, to provide fairness.

3 Trust as a Fairness Parameter

In this section we start by providing a few notions related to *social trust* modeling, as trust as a QoE parameter has roots in social sciences paradigms.

In UCNs, a node i is defined to be a (wireless) device that belongs to an entity, its *owner*. An owner can be a specific user, or a group of users. In terms of trust and assuming that a networked device can be shared by different users, only the owner is responsible for such device. In other words: the trust computation, negotiation, and establishment is always associated to the owner identifier, and not to the device. Moreover, an owner may be responsible for more than one node. Nodes are associated to other nodes by means of trust associations.

A *trust association* is the k-th directed association between two nodes and is related to the respective owner's interests and social networking perspective. A trust association holds a cost, the *trust level*. The trust level provides a measure of previous trust behavior which can be considered as a QoE parameter. The rationale for this assumption is that a user is more willing to share resources within its trust circles. The computation of a trust level derives from each owner trust expectations and beliefs. Furthermore, such computation takes into consideration local and external influences. Examples of local influences are the degree of connectivity and reputation level of a node. External influences are influences that do not relate to the nature of each node but to external networking conditions (e.g. too much overhearing probability around a node).

Two nodes may hold more than one trust association among them, for instance, one per specific service. In this paper we consider a trust association to be unique and unidirectional between two nodes. Hence, a trust association from node A to node B may or may not have a different trust level than a trust association from node B to node A.

3.1 Examples of Operation

To better explain the notions behind trust as a social parameter that can be applied to networking this section provides a description of a few operational examples. For the given examples we consider that trust levels are deterministic and based on the values provided in Table 1. Such trust level representation is here provided for illustration purposes only. In a real environment the trust levels can be computed dynamically based on common reputation or recommendation schemes, as explained in section 4.

Table 1, exemplifies a potential mapping of trust levels to service levels to be provided, i.e., a direct translation between QoE and QoS levels. A trust level of zero from node A to B ($T_{AB} = 0$) means that there is no trust association, which is reflected in the absence of data from A to B. When the level is set to 0.1, it means that a trust association has been recently established and that node B is in quarantine mode, i.e., node A will only transmit data to B that does not require confidentiality. A trust level of 0.3 is sufficient to allow node A to send data to node B. Such data although not confidential requires reliable treatment by node B. A trust level of 0.3 allows node A to send confidential data to node B, while a level of 0.6 means that nodes belong to a closest list of trusted devices bringing extra guarantees to node A beside confidentiality, such as non-repudiation and privacy by node B. When the trust level is negative it means that there is good evidence that node B has been misbehaved, which means that such node may be subjected to a penalty, such as getting lower priority when accessing the Internet.

Table 1: Illustrative trust level categorization.

Trust Level	**Meaning**	**Action**
-0.1	Misbehaved user	Penalty
0	Not trusted	No data exchange
0.1	Recent acquaintance, quarantine mode	Only data that requires no confidentiality
0.3	Sufficient trust level	Node trusts enough to send data that is not confidential but requires reliability
0.6	Good trust level	Confidential data can be exchanged
1	Fully trusted	Closest list of trust

Let us now consider the scenario illustrated in Figure 1 where it is assumed that there is an already established community composed of three nodes (A, B, MP). Each node holds a trust table where each entry includes an index, trust level, as well as an aging value in seconds. The node MP holds two trust associations (1 and 2) towards node A (T_{MPA_1} and T_{MPA_2}), and one trust association towards node B (T_{MPB}). Both A and B are fully trusted by the MP that allows them to access the Internet with guarantees of non-repudiation. However, the MP only allows data originated from nodes adjacent to A to reach the Internet within a trust level of three, which means that the MP may impose some extra security mechanism to such traffic, such as tagging packets with an alert label. Each trust association entry is refreshed after 100 seconds, as illustrated in the figure.

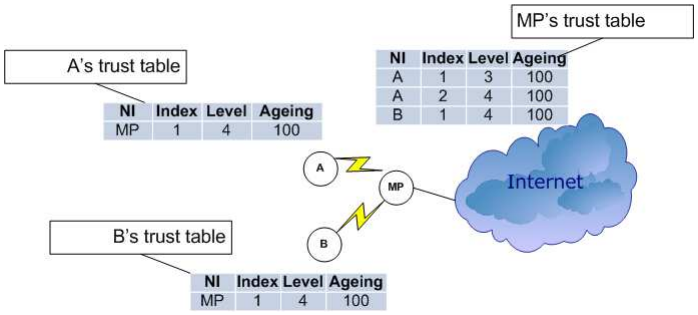


Fig. 1: Operational example for a community with three nodes: A, B, the MP.

Let us now consider that a new node C recently registered in the community wants to access Internet. C is known to B - has a trust association to B - but not to A. When it tries to connect to the MP node C triggers a request for trust recommendations. This request has two purposes: i) to check the reputation of the MP in the community; ii) to ask neighboring nodes to recommend MP.

Both nodes A and B reply to C stating that they have good trust level associations towards node MP by sending the respective trust levels and hence node C places a new trust association towards the MP in its trust table, weighting its own beliefs (e.g. a weight) and the answers from the neighboring nodes. The computation of such weight would e.g. result in a trust level of 4.

At the same time, the MP broadcasts a request the network to collect recommendations about C. Let us first assume that node B knows C (has a trust association with C on level 3). Node B replies with this level to the MP, which accepts node C, creating a trust association of level 1, based on its own expectations and the provided answer. Node A claims that it does not know the node (answers with a trust level of 0). Depending on the answer of other nodes and on the node C behavior, the MP may or may not change the trust association level towards C.

Let us now consider that node C is not known by any node on the network. The MP gets no answer but based on its own willingness to share (belief concerning how to deal with unknown nodes) accepts the connection but places node C on trust level 0.1 - quarantine.

3.2 Background on Trust Management

To provide a perspective on how the global trust framework works on UCN this section provides a description of the general functionality of the trust management scheme. For the remaining sections we shall consider the role of a *requestee* or of a *requester* in trust negotiation. A *requestee* in UCN corresponds to the notion of gateway (normally, an Acess Point). While the *requester* role can be assumed by both a node and a gateway: nodes perform trust negotiation towards gateways; gateways perform trust negotiation among themselves.

During boot up of the nodes, there are a few steps related to the initial setup of trust parameters, i.e., the way that nodes perceive others around, when they are in untrusted environments. Since the UCN trust environment may not be enough as an incentive for cooperation, the boot up phase ends up with the assignment of a set of *credits* that the requester may use to access shared resources. Based on the collected information the requester will try to establish trust associations with one of the responsive gateways and the MAC association part is established upon a successful end of trust negotiation.

Therefore, trust negotiation and initial credit assignment [13] are crucial to allow a node to associate with a gateway in UCNs. Full details concerning a model for trust management in UCN is out of the scope of this paper. The reader can find more information in Chapters I and II.

3.3 Applying Trust to QoS, Tokens as a Translation Currency Unit

In the previous section we have discussed and explained notions concerning how trust, which is a social parameter derived from human beliefs and interests, can be used as a QoE parameter to increase resource management fairness. As it is a social notion, trust is too subjective to be applied directly to networking. We consider trust weights to be values between 0 and 1, following the recent trends in distributed trust schemes. Trust, however, as a QoE parameter, cannot be used directly to improve the network performance and in particular fairness, as by simply considering trust levels, users that are more trusted would become greedy users and consume all of the resources in the network. Hence, to apply trust in the context of QoS it is necessary to consider incentives which motivate a good behavior, together with trust levels. In current UCNs users share Internet access in exchange of broader roaming. The network utility considered here is connectivity. However, there are additional networking resources that can be shared in exchange of other benefits. For instance, a user that cooperates frequently by opening its access points can be rewarded later not necessarily with the same type of service, but with a local service (e.g. access to a local printer in an airport; profiting from a relay in an area where the device does not have direct communication to any access point).

To make such exchange truly fair, we consider that resource assignment is based on the combination of trust associations and *credits* a node is willing to spend to get a service. Based on these two parameters, we consider a unique and virtual currency in the form of a *token*: a token is therefore a virtual measure (unit) of resources. Such a virtual currency allows for a direct exchange of different goods even in different instants in time.

Tokens are, as mentioned, the result of a utility function which has as input both a trust level of an association between two nodes, and a set of credits that a node is willing to spend to get a specific service. Such a function should take into consideration higher trust levels but also larger sets of credits. However, we expect it also to vary slowly and to depend more on the trust level, than on credits, as credits are an item that can be acquired and could lead easily to greedy situations. In other words, if the trust weight for a specific association between

two nodes (*requestee* and *requester*) is low then even if the node requesting credits has a high credit level, the resulting token value should progress slowly. While if a requester - Requestee association shows a good trust level, then if it uses a high level of credits, the resulting tokens should also not increase linearly, as this would make the node consume all of the available resources.

To exemplify this line of thought, we consider two different functions to consider as provided in Eqs. 1 and 2.

$$tk(i,j) = tl(i,j) * \sqrt{c}, tl \in [0,1]; c \in [0,\infty] \quad (1)$$

$$tk(i,j) = tl(i,j)^{\log(c)}, tl \in [0,1]; c \in [0,\infty] \quad (2)$$

The main differences between Eqs. 1 and 2 are illustrated via Fig. 2. This figure shows two charts. (a) corresponds to Eq. 1, and (b) to Eq. 2, where values for the trust level tl and credits c have been varied to exemplify the impact on the computation of tokens.

Eq. 1 (cf. Fig. 2 (a)) is a utility function that results in a token progression that follows both credit and trust level growth. If by some reason the trust level is decreased (the user is penalized) then so are tokens, independently of whether or not the user has a large amount of credits. This function prevents greedy and misbehaving users to get a hold on all of the resources of the network, as tokens are to be exchanged by resources.

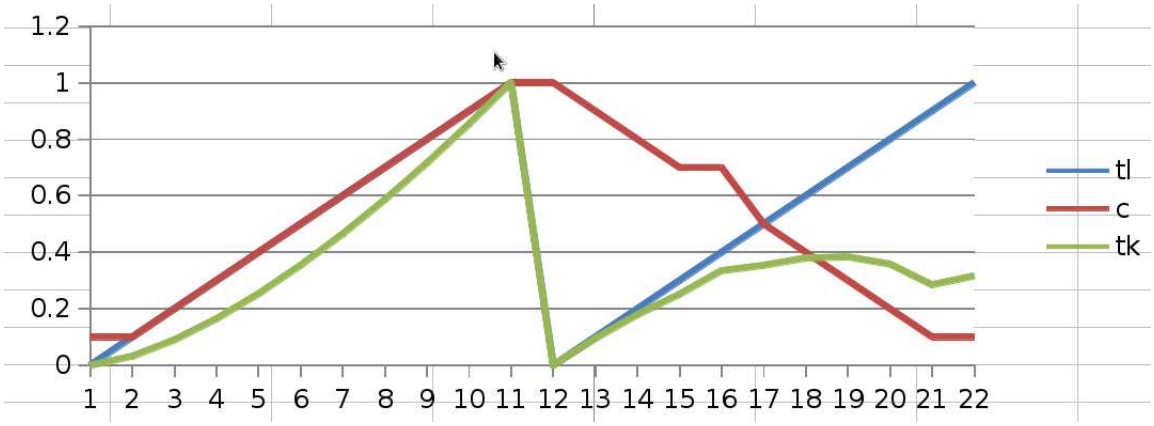
Eq. 2 (cf. Fig. 2 (b)) results in a larger number of tokens when credits and trust level is low, but with the increase on both these parameters, the resulting tokens also increase. The function is not so sensible to misbehaving users.

The functions here provided are discussed to explain how tokens can be defined to dynamically allow the translation between a social parameter such as trust, and networking resources.

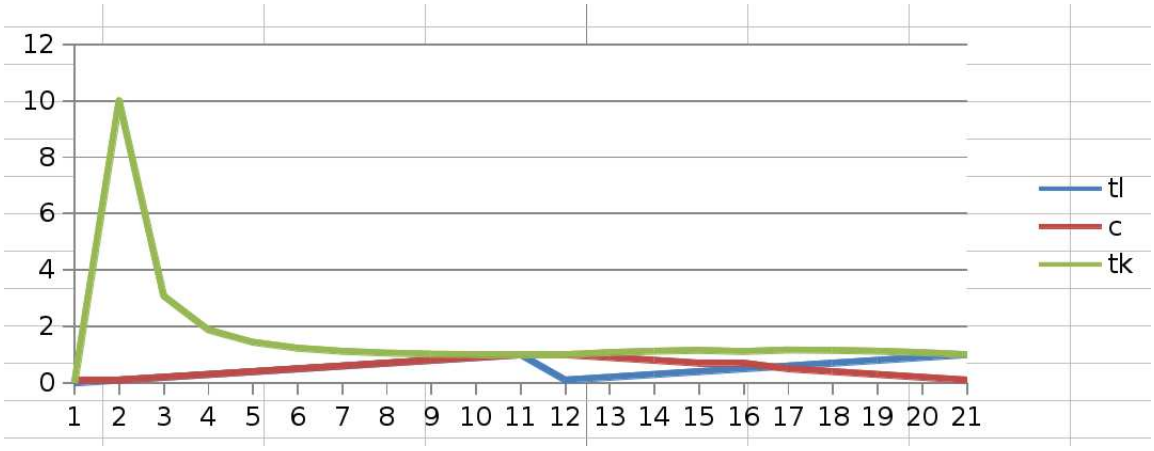
The next section describes an example on how trust, and tokens, can be applied in the specific context of resource management, to call admission control, with the motivation to increase fairness in wireless networks and as a consequence, to improve user satisfaction.

4 Call Admission Control Based on Trust Circles

The description provided in this section is based on the UCN model provided by the European project ULOOP. The main blocks of a UCN have been described in Chapter I [13]. In ULOOP, resource management relates to self-organization and cooperative aspects, which are addressed from an OSI Layer 2 and Layer 3 perspective. Resource management aspects in ULOOP comprise a block which is divided into four main sub-blocks which are described in this chapter. In what concerns *Call Admission Control* (CAC), this is a functional block which takes care of prioritizing requests based on both network conditions as well as on trust levels that the users (and consequently their owned devices) have in the network, towards networking devices. CAC starts prioritizing and queuing



(a) Eq. 1 variation based on credits and trust levels.



(b) Eq. 2 results variation based on credits and trust levels.

Fig. 2: Examples for token definition based on trust levels and credits

incoming requests so that contending requests can be treated based not only on the network conditions, but also on the trust association that a gateway (its owner) has towards a device (its owner). Queued requests are handled based on another thread, again related with prioritization as well as feedback from a resource allocation sub-module.

Incoming requests are classified by ULOOP gateways as "known" (e.g. flag Known=1) or new (e.g. flag known=0) as a way to prioritize requests from nodes that the gateway has recently authorized. A "Known" request example can be a request from a node that has just been served by this gateway e.g. 30 seconds ago, or a node that has been accepted to be transferred to this gateway by a gateway in the vicinities.

CAC then takes care of prioritizing requests according to a specific utility function that considers the trust level of the gateway towards the node, as well as the number of tokens that the node wants to exchange for a specific service. An example for such a function is provided in Eq. 3, where p corresponds to the priority which is proportionally dependent on the tokens that node i provides to j, to apply for a specific service, and dependent on the trust level that node j has on node i.

Moreover, the gateway checks whether or not it is a suitable gateway to handle the request. This is done based on local information that CAC can periodically collect from feedback of neighboring gateways. Assuming a case where the gateway decides it cannot serve the request or that there is a more suitable gateway, then the gateway redirects the request to that gateway, directly to the node, by providing the MAC of the best gateway.

Assuming a gateway that can serve a specific request, then CAC simply redirects the request to the resource allocation module.

$$p = tk(i,j) * tl(j,i) \tag{3}$$

5 Summary and Future Work

This paper addresses the applicability of trust metrics as a fairness parameter in call admission control within the context of user-centric networks. The paper explains how trust can assist in improving user Quality of Experience in wireless networks, by taking into consideration not only channel conditions, but also trust levels derived from the interaction that users have in the context of Internet shared services.

References

1. The Haggle Project. Code available at: http://code.google.com/p/haggle/
2. R. Sofia, P. Mendes, “User-provided Networks: Consumer as Provider”, in IEEE Communication Magazines Feature Topic on Consumer Communications and Networking - Gaming and Entertainment. 2008.
3. M. H. Ahmed. "Call admission control in wireless networks: A comprehensive survey." IEEE communications Surveys and Tutorials 7.1-4 (2005): 50-69. 2005
4. F. Yu, V. Leung. "Mobility-based predictive call admission control and bandwidth reservation in wireless cellular networks." Computer Networks 38.5 (2002): 577-589. 2002
5. T. Kwon, S. Kim, Y. Choi, and M. Naghshineh. "Threshold-type call admission control in wireless/mobile multimedia networks using prioritised adaptive framework." Electronics Letters 36, no. 9 (2000): 852-854.
6. Y. Xue, L. Baochun, K. Nahrstedt. "Price-based resource allocation in wireless ad hoc networks." Quality of Service—IWQoS 2003. Springer Berlin Heidelberg, 2003. 79-96.
7. K. Piamrat, A. Ksentini, C. Viho, and J-M. Bonnin. "Qoe-aware admission control for multimedia applications in ieee 802.11 wireless networks." In Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th, pp. 1-5. IEEE, 2008.
8. D. Pong, T. Moors. "Fairness and capacity trade-off in IEEE 802.11 WLANs." Local Computer Networks, 2004. 29th Annual IEEE International Conference on. IEEE, 2004.
9. M. Ivanovici, R. Beuran. "Correlating quality of experience and quality of service for network applications." Quality of Service Architectures for Wireless Networks: Performance Metrics and Management (2010): 326-351.
10. Z. Fang, B. Bensaou. "Fair bandwidth sharing algorithms based on game theory frameworks for wireless ad-hoc networks." INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies. Vol. 2. IEEE, 2004.
11. M. J. Neely, "Optimal pricing in a free market wireless network." Wireless Networks 15.7 (2009): 901-915.
12. J. Zhang, N. Ansari. "On assuring end-to-end QoE in next generation networks: Challenges and a possible solution." Communications Magazine, IEEE 49.7 (2011): 185-191, 2011.
13. R. Sofia, User-centric networking: bringing the Home Network to the Core. Springer LCNS User-centric Networking - Future Perspectives, To Appear, 2014.
14. R. Sofia, P. Mendes, M. J. Damásio, S. Henriques, F. Giglietto, E. Giambitto and A. Bogliolo, Moving Towards a Socially-Driven Internet Architectural Design (2012), in: ACM SIGCOMM CCR Newsletter, 42:3. 2012.