Extending Trust Management with Cooperation Incentives: Achieving Collaborative Wi-Fi Sharing Using Trust Transfer to Stimulate Cooperative Behaviours

Carlos Ballester Lafuente, Jean-Marc Seigneur

Extending Trust Management with Cooperation Incentives: Achieving Collaborative Wi-Fi Sharing Using Trust Transfer to Stimulate Cooperative Behaviours

Carlos Ballester Lafuente[1], Jean-Marc Seigneur[1]

[1] University of Geneva, ISS & Medi@LAB, GSEM & SdS, CUI
7 route de Drize, Carouge CH1227, Switzerland
Carlos.Ballester@unige.ch, Jean-Marc.Seigneur@reputaction.com

Abstract. There are still many issues to achieve collaborative Wi-Fi sharing: the legal liability of the sharer; high data access costs in some situations (mobility when going over a monthly subscription quota, roaming…); no appropriate incentives to share. Current trust management could exclude the malicious users, but still could not foster Wi-Fi sharing. We have extended an appropriate trust metric with cooperation incentives to mitigate all the above issues. We have evaluated our proposal with a trust metric and incentive effectiveness through simulations and we have found the bootstrapping time for such a system and the average depletion time for its users linking it with the size of the system's user base, proving the feasibility for such a combination.

Keywords. Wi-Fi, collaborative sharing, trust, cooperation incentives, trust points.

1 Introduction

According to the International Telecommunication Union (ITU) [1], the number of subscribers using mobile broadband Internet services has raised from 268 million in 2007 to an impressive 2.1 billion users in 2013, accounting for more than the 50% of the world's Internet usage.

This previous fact and the emergence and fast growth of applications such as social networking, user generated content, location services, collaborative tools, augmented human and augmented reality applications etc., has fueled the user's need for permanent connectivity wherever she/he is, and under all circumstances. While in regular day-to-day environments this need can be fulfilled with regular wireless access provided via hotspots (wireless access points) or mobile data transmission technologies such as 2G, 3G, HDSPA, UMTS, etc., situations on which the user is a) roaming (does not have access to his mobile operator because of being in a different country), b) out of the area of network coverage or c) has already consumed her or his monthly data allowance, might deter the user to connect through such previous mentioned mobile technologies, as the cost can be very high. These three previous reasons make connectivity through

regular means to be difficult to attain, thus impeding the use of such smart mobile applications, augmented reality applications, or the mere upload of data and statistics for user tracking or measuring purposes.

In order to solve such a challenge, we have envisioned a collaborative wireless access sharing. Simply put, locals to the environment become mobile hotspots on the fly, sharing their mobile data access, via their personal mobile hotspot in their device, with a foreigner for the (rather short or not) period of time that they might be in range. In this way, all the users that are either roaming or with no access to mobile data are still able to upload fundamental data and statistics and even use applications on places where normally they wouldn't be able to get connectivity through their own means or would be too expensive to do so. All of this, without having to deploy real fixed wireless access points and signal amplifiers, and not limiting the area of coverage, as the access points are carried by the local people, which might be static or on the move.

In such scenarios where several strangers are expected to interact for the sake of data transmission, trust and cooperation incentives are of vital importance to ensure the robustness and reliability of the overall system. Cooperation incentives can be used to complement and collaborate with trust management as users can benefit from them while using the system, thus encouraging user's good behaviour. By providing cooperation incentives, there are economic dynamics involved, encouraging the users to keep using the system in a rightful way as they benefit from it. This in turn, encourages the user to earn a good trust level, as other users are more likely to interact with highly trusted users than less trusted ones, reinforcing the trust system.

In this paper, we present how we integrate trust management and cooperation incentives with our collaborative wireless access sharing service, being the aim of the paper to evaluate the computational trust management and cooperation incentives working together and to obtain results about its feasibility.

The rest of the document is organized as follows. First, section 2 presents the current issues on collaborative Wi-Fi sharing, and following, section 3 describes how the related work has tried to tackle these issues. After, section 4 presents the trust management and cooperation incentives framework. Next, section 5 shows the simulation, and the results obtained from it. Finally, section 6 concludes the paper.

2 Current Issues

There are many issues related with Wi-Fi sharing and accessing mobile data that need to be addressed in order for a collaborative Wi-Fi sharing service to be as useful and reliable as possible. Following we detail the most important points to be addressed.

2.1 Legal Liability of the Sharer

One of the biggest concerns with Wi-Fi access sharing is that all the data traffic goes out from the same source – the wireless router or access point – rendering the owner of the device liable for any action that any user with whom she or he has shared the access

with has performed, illegal content download, malicious actions taken against any entity or any other legally punishable action.

This legal liability might deter many users from sharing their Wi-Fi or other type of data access, thus making it difficult for a service of this kind to succeed. In our collaborative Wi-Fi sharing service, we address this issue protecting the sharer against legal liability by putting into play some protection mechanisms. These mechanisms and their internals are out of the scope of this paper, that focuses on the computational trust management and cooperation incentives used in addition to these legal aspects mechanisms.

2.2 High Roaming Costs

As stated before, roaming costs incurred by users when operating their smartphones in another country, and also extra costs derived from going over a certain monthly data allowance for local users might deter those users from using any application or accessing data when on that situations.

High roaming costs make the access of mobile data while abroad very expensive, and thus, impede users to access applications and other online sources normally, as the price they might pay in order to use these services would escalate very quickly. A recent study on international roaming costs [2] carried out by the OECD, sets the average price per MB when roaming in the EU/EEA area at an average of 2.60€. This is likely to change in the future given that the EU is pushing to eliminate the roaming costs (or most of them), even though our assumptions remain valid up to today and the next years, plus roaming would still exist outside the EU.

With our collaborative Wi-Fi sharing service, we want to overcome the problem of high roaming and monthly allowance surpass costs, allowing users who are not in their home country or who have depleted their monthly quota in their home country to still be able to obtain connectivity through collaborative Wi-Fi sharing.

2.3 Lack of Cooperation Incentives

Even though all these previous issues were to be solved, one last issue affecting in general peer-to-peer and sharing services still remains. The “Tragedy of the Commons” [3] states that it is unavoidable in the human nature the depletion of a shared resource by individuals, acting independently and rationally according to each one's self-interest, despite their understanding that depleting the common resource is contrary to the group's long-term best interests. Even though the tragedy of the commons was first applied to mainly economic and sociology fields, it can be extrapolated to P2P and other sharing services as can be seen in [4] and [5].

Without a strong incentive being present, there is no real reason for users to share back as much at least as they got available when some other user shared, as it is in the very human nature to be self-interested agents, thus acting exclusively for their own benefit. This lack of incentives will ultimately render the service unusable, as there will be no resources to share, but many users willing to use shared resources. In our service, we solve this problem by integrating cooperation incentives with trust management as explained in following sections.

3 Related Work

In this section we present the closest work to ours, both regarding trust and cooperation and similar systems and architectures.

3.1 Trust and Cooperation

The need of cooperation incentives to strengthen trust management on cooperative systems has been already the issue of discussion of several papers.

In Fernandes et al. [7] the authors introduce a framework to provide incentives for honest participation in trust management infrastructures. The aim of their system is to improve the quality of information provided by reducing free-riding and fostering honesty. In order to achieve this, they use two strategies: i) to provide rewards for participants that advertise their experiences to others, and ii) to impose the credible threat of stopping the rewards for participants who consistently provide suspicious feedback. In the paper they successfully prove that this two aforementioned measures effectively works as an incentive that strengthens the underlying trust metric, deterring participants from cheating or misbehaving.

In Bogliolo et al. [6] the authors argue that the success of user-centric networks strongly depends on the willingness of the participants to cooperate. Incentives can help in encouraging users to cooperate and reputation-based incentives and remuneration are proposed to increase users' motivation and to discourage selfish behaviors. Quantitative properties of cooperation incentives are defined and analyzed through model checking. Their model considers users providing services, which are called requestees and users receiving services, which are called requesters. The model presents four phases of cooperation: i) discovery and request ii) negotiation iii) transaction and iv) evaluation and feedback. Their reputation system defines cooperative attitude, which depends on dispositional trust and service trust level, which represents the threshold under which the service is not accessible. The authors also introduce a virtual currency system where reputation-based and reward-based incentives are combined by including the trust level of the requestee towards the requester as a parameter affecting the cost of the negotiated service. Finally, they prove through Markov decision process analysis that mixing incentive strategies such as reputation and reward proves effective in inducing pro-social behaviors. Also they prove that cooperation incentives favor both requester and requestee as honest requesters get services at a lower price and reputation and cooperative attitude impact earnings in requestees.

3.2 Similar Systems and Architectures

There are other systems that aim to provide connectivity through sharing in order to tackle the same or similar problems. Here we describe them and we present how they address the issues explained in the previous section.

Open Garden.

The Open Garden application [8] enables users to access the most appropriate connection without configuring their devices or jumping through hoops. It also enables users to access Internet as cheaply as possible. Users can find the fastest connection and most powerful signal without checking every available network, and can move between networks seamlessly. Open Garden provides a way to access more data at faster speeds in more locations. Consumers actually become part of the network, sharing connections when and where they provide the best possible access. The service is still quite new and many features have not been thoroughly reviewed by real users, though it is complicated to assess the veracity of the authors' claims.

Legal Liability of the Sharer.

Open Garden does not address the problem of the sharer being legally liable over the actions that any user connected to her or his Wi-Fi network might undertake.

Strong Authentication of the Client.

Open Garden aims for seamlessly connectivity without the intervention of the user. It doesn't authenticate the clients or sharers in any possible means and connections are made automatically without any initial configuration or authentication step.

Mobile Data Limits.

No possibility to set any limit, thus no control over how much data is shared risking the danger of going over a certain monthly quota.

High Roaming Costs.

By offering seamless connectivity between devices allowing easily the sharing of a Wi-Fi connection over 3G or 4G data, Open Garden effectively addresses the problem of high roaming costs, as foreign users can connect to other local users through their on the fly mesh network and obtain data access at no cost for them.

No Incentive.

Open Garden does not yet offer any incentive in the form of credits or rewards. However, it plans to use some form of credits based on what can be seen on their Web site.

ULOOP.

The ULOOP [9] FP7 European project brings in a fresh approach to user-centricity by exploring user-provided networking aspects in a way that expands the reach of a multi-access backbone. ULOOP addresses the user as a key component of networking services in future Internet architectures. Building upon current (commercial) examples ULOOP explores not only the adequate technical sustainability of user-centric models, but also legislation implications and the potential of community-driven services and how these new aspects may give rise to novel business models both from a user and from an access perspective. The aim of ULOOP if to seamlessly expand the backbone

of the network through the end users' devices, extending the area of coverage while offloading the often saturated provider networks.

Legal Liability of the Sharer.
ULOOP does not address the problem of the sharer being legally liable over the actions that any user connected to her or his Wi-Fi network might undertake.

Strong Authentication of the Client.
ULOOP assumes worldwide strong authentication of any user: a ULOOP user cannot be given more than one ULOOP digital identity. Also it puts in place a trust metric, but the metric does not need to be as attack-resistant as a unique digital id given per user worldwide is assumed in ULOOP.

Mobile Data Limits.
No possibility to set any limit, thus no control over how much data is shared risking the danger of going over a certain monthly quota.

High Roaming Costs.
By seamlessly expanding the backbone of the network through the end users' devices, extending the area of coverage while offloading the often saturated provider networks, ULOOP addresses the issue of high costs while roaming as any ULOOP node can connect to a ULOOP gateway and after some negotiation steps it will have access to the Internet through it.

No Incentive.
ULOOP provides cooperation incentives in the form of credits, which can be gained while acting as a gateway and providing services to other ULOOP nodes and can be spent while acting as a node when requesting services from a gateway.

Air Mobs.
Air Mobs [10] is an application that enables users to share their excess data with users who might be running up against their monthly limits. Essentially, one user agrees to let their mobile device act as a tethering hub that will send data from their LTE smartphone over Wi-Fi to any users nearby. In exchange, the central hub user gets a "data credit" that gives them access to other users' data in the future. Put another way, the new app creates a sort of "cap-and-trade" market for mobile data that helps users exceed the hard limits set on their consumption by rationing data with one another based on their needs at given times.

Legal Liability of the Sharer.
Air Mobs does not address the problem of the sharer being legally liable over the actions that any user connected to her or his Wi-Fi network might undertake.

Strong Authentication of the Client is Still Difficult.
Air Mobs does not provide any means of authentication.

Mobile Data Limits.

Air Mobs monitors network connectivity and status in order to give the user the ability to control how much of her data plan she is willing to share, making sure other users cannot use more data than the amount designated by the owner of the hosting device.

High Roaming Costs.

Air Mobs provides network connectivity when one device has no available Internet connection or roaming costs are too high, thus tackling effectively this problem.

No Incentive.

Air Mobs creates incentive via a secondary credit market –a user will be willing to share her or his data connection since she or he will get data in return.

3.3 Summarizing Table

Following, we summarize all the previous characteristics of Open Garden, ULOOP and Air Mobs in the form of a table, in order to ease the comparison between them. The information on which of the issues each of the services address can be found in Table 2.

Table 1. Current issues on Wi-Fi sharing addressed by each system.

Issue	Open Garden	ULOOP	Air Mobs
Legal liability	X	X	X
Authentication	X	√	X
Mobile data limits	X	X	√
Roaming costs	√	√	√
Incentives	√	√	√

4 Trust and Cooperation Incentives

The aim of this section is to describe in detail the main components of our model, namely the trust management metric and the cooperation incentives.

4.1 Trust Transfer

Trust transfer [17] has been proven to protect against Sybil attacks when pieces of evidence are limited to direct observations and recommendations based on the count of event outcomes. Trust transfer implies that recommendations move some of the trust-

worthiness of the recommending entity to the trustworthiness of the trustee. This approach is particularly efficient for our system, as besides assessing trust we can use the metric to reward in the form of trust points the agents that share their Wi-Fi connectivity, effectively combining trust management with cooperation incentives as will be explained in following sections.

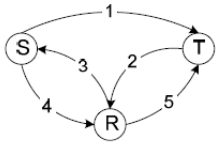

Fig. 1. Trust Transfer process.

Based on Fig. 1, Trust Transfer works in the following manner:

1. The subject requests an action, requiring a total amount of trustworthiness TA in the subject, in order for the request to be accepted by the trustor.
2. The trustor queries its contacts, in order to find recommenders willing to transfer some of their positive event outcomes count to the subject. Trustworthiness is based on event outcomes count in trust transfer.
3. If the contact has directly interacted with the subject and the contact's RP allows it to permit the trustor to transfer an amount of the recommender's trustworthiness to the subject, the contact agrees to recommend the subject. It queries the subject whether it agrees to lose A of trustworthiness on the recommender side.
4. The subject returns a signed statement, indicating whether it agrees or not.
5. The recommender sends back a signed recommendation to the trustor, indicating the trust value it is prepared to transfer to the subject. This message includes the signed agreement of the subject.

4.2 Cooperation Incentives

Trust Transfer can be easily and effectively integrated and turned into cooperation incentives, as the trust points that are transferred can be used as a sort of "virtual currency" in order to exchange them against provided services, in this particular case, Wi-Fi connectivity. In this subsection, we explain both which the cooperation incentives in place are and how to extend them and make them more attractive through friend-of-a-friend (FoaF) chains.

Basic Incentives

In order to foster interaction amongst users in a collaborative environment such as the one described in this paper, there is a need to offer incentives to the users besides providing them with the appropriate safety features such as a solid trust metric.

Trust Transfer can effectively be used as a cooperation incentive enabler, by using its trust points as the de facto "currency" in order to be able to use the services other

users have to offer, in this case Wi-Fi connectivity sharing. By awarding trust points to the service provider proportionally to the duration of the Wi-Fi sharing period, we foster cooperation among users as not only the trust points reflect the good behaviour of the user giving her a good reputation, but also enable her to in turn obtain Wi-Fi connectivity when roaming or being out of data by using those trust points earned previously in order to pay for the service.

The more you share in the system, and the more different users you share with, the easiest will be to in turn find another user which will accept your trust points as payment, be it because of having interacted directly with her or using trust transfer mechanisms to find another user who can lend the service requester those needed points as explained in the previous section.

We reckon that these incentives are limited by your own circle of direct interactions and acquaintances inside the system, and this is why we exploit another capability of trust transfer, which is being able to transfer trust points through chains of trust with multiple hops, as explained in the next subsection.

Small World Network Subsets

To empower the cooperation incentives provided by Trust Transfer and the trust points, some other mechanism in order to extend the usefulness of those points needs to be introduced, as Trust Transfer contemplates mainly that trust points are to be used "one-to-one", or as most with one degree of indirection. This means that in a scenario where several strangers are supposed to cooperate and to share services, it would be difficult to spend those points as the likeliness of finding in the same environment another user which one has already interacted with, or as most within one degree of separation is highly unlikely.

In order to overcome this limitation, we have explored the probabilities of finding longer "friend-to-friend" chains, applying the principles of small worlds [11] and degrees of separation. For the sake of simplicity, we assume that most of the system's users come from networks which are already highly connected, such as Facebook.

Social Networks like Facebook have been proven to have a degree of separation of around 4.76 to 6 with almost a 100% of probabilities [12, 13]. The problem of finding the probabilities for a subset of a small world network to find a chain of 6 degrees of separation or less can be modelled as random node failures (different from targeted attacks) in the complete network until we are left with the desired amount of nodes, which would be our subset of the small word network. In order to model a social network like Facebook, we need to use a scale-free network which exhibits both short paths and high clustering degree. Such a network can be modeled by using a KE (Klemm and Eguíluz) [14] Network, which is a type of scale-free network which complies with both properties.

While the most used metrics to determine the properties of a network are L (characteristic path length) and C (clustering), those can produce misleading results when used to re-evaluate such properties when eliminating large portions of random nodes, as disconnected or isolated users or small unreachable clusters can skew the results. It is thus a better estimate of the properties of a network, as stated in Crucitti et al. [15], the one produced by the global and local efficiency (E_{glob} and E_{loc}). The efficiency of a network

is defined as the effectiveness of the network to propagate information both globally and locally, meaning the possibility of finding a path in between two nodes of that network for the information to propagate. Those definitions can be modelled mathematically as seen in Fig. 2.

$$E_{\text{glob}}(\mathbf{G}) = \frac{\sum_{i \neq j \in \mathbf{G}} \epsilon_{ij}}{N(N-1)} = \frac{1}{N(N-1)} \sum_{i \neq j \in \mathbf{G}} \frac{1}{d_{ij}} \qquad E_{\text{loc}}(\mathbf{G}) = \frac{1}{N} \sum_{i \in \mathbf{G}} E(\mathbf{G_i})$$

Fig. 2. Global and local efficiency on a network.

Taking this formula into account, and applied over a network inducing random failures and targeted attacks, the authors in [15] have come up with the results that can be seen in Fig. 3.

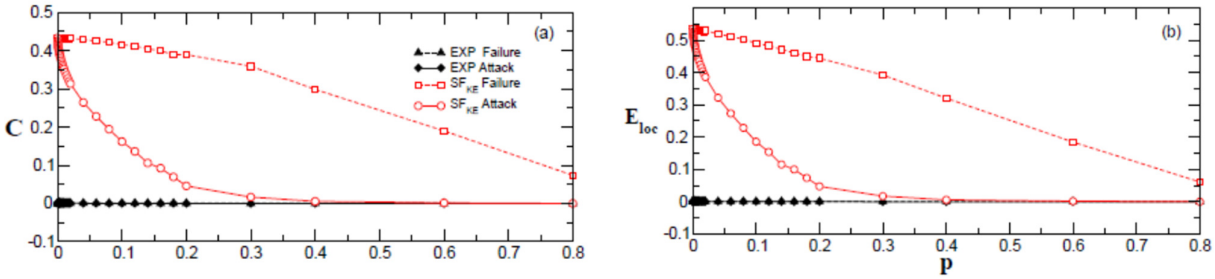

Fig. 3. Clustering and efficiency loss for percentages of random failure in nodes and targeted attacks [15].

As we have seen in the previous graphs, until the network is not at least a 20% of the original, the efficiency or clustering size is not big enough to even consider it a functioning network. Nevertheless, there are other aspects that have not been taken into account in the purely mathematical demonstration:

- Facebook is especially high clustered (much more than any of the networks in the previous results), to which one could argue that the removal would not impair the network as badly as that.
- When users decide to adopt a system which is collaborative and based in friendships, most likely it will be adopted in an «epidemic» way, on which friends and friends of friends would install it, leading to an also highly clustered and connected sub-network.
- The interactions between disconnected users while using our system, would in the long run create a small world by itself.

In our simulations, we apply these same principles and we calculate for a given user base population, how quick the full system would bootstrap and which is the minimum

amount for such a user base which would enable reasonable probabilities of finding such FoaF chains so the cooperation incentives are more useful and in turn, encourage the users to cooperate and behave properly.

5 Evaluation

In this section, we proceed to present the details of the simulation environment, and the results obtained from running those simulations, both in terms of bootstrapping time and user data depletion times.

5.1 Simulation Environment

The model has been simulated using AnyLogic [18]. AnyLogic is a simulation tool that supports System Dynamics, Process-centric (Discrete Event), and Agent Based modeling, based on the Eclipse platform. The flexibility of its modeling language provides the opportunity to capture the complexity and heterogeneity of a given system to any desired level of detail, and its object-oriented model design paradigm provides for modular, hierarchical, and incremental construction of large models. The simulation environment corresponds to a real world area, which is the airport of the city of Geneva, Switzerland. The environment has been modeled respecting the real dimensions of the airport, and also the real proportions of both local and foreign travelers and permanent workforce of the airport [16]. The exact details of the simulation are as follows:

- 450 meters long and 150 meters wide, spanning 3 floors of this same size
- Around 13 million passengers in 2012, from which 55% are foreigners and 45% are locals.
- 840 staff and permanent workers (working in shifts).

Taking into account this previous data, each of the simulation runs has been done with 3000 agents which simulate passengers (both local and foreign in the proportions previously mentioned) and 280 workers (assumed always locals) at any time, included in those numbers. To make the scenario as realistic as possible, agent renewal happens with a normal distribution with an average of 2 hours in order to simulate the passengers leaving and new ones arriving. Workers are also renewed in 8 hour shifts. We assume that locals have an average of 15-20 friends (acquaintances or previously interacted users) and foreigners an average of 2. All local workers are known to each other.

5.2 Simulation Results

In order to study the feasibility of the system, we have run several simulations each with a different user base for the system. This user base is a key point, as it will determine the threshold from which the system might be usable both from the bootstrapping point of view and from incentives perspective. Note that when we talk about user base (or system users), we are not talking about the amount of agents in the simulation, which are fixed according to the criteria mentioned in the previous section, but to the total

amount of users in the world using this system. This user base is what enables the probabilities of finding long FoaF chains in order to enhance the cooperation incentives provided by Trust Transfer. Each simulation runs for a real-world whole day, measured in seconds (86400 seconds)

Bootstrapping Measurements

For the system to be usable, the bootstrapping time needs to be as low as possible in order for the foreigner passengers to be able to connect to locals while in their short time at the airport. We consider that the system is bootstrapped if half of the agents that can provide connectivity have successfully shared at least once their Wi-Fi with a foreign or a local agent that might have run out of data. For each of the graphs presented below, the Y axis represents amount of agents and the X axis simulation time, measured in seconds. We have run the simulation for different sizes of user base population, ranging from 2 million system users to 200 million system users with an intermediate simulation accounting for a 20 million system user base. The results can be seen in Figs. 4-6.

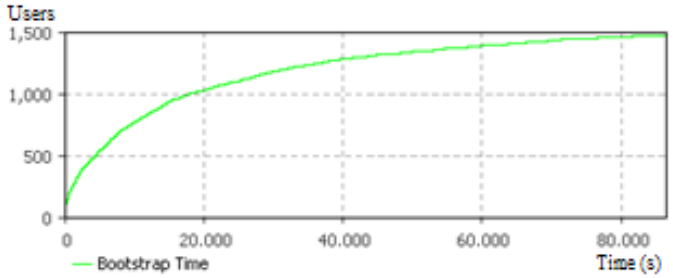

Fig. 4. Bootstrap time with 200,000,000 system users worldwide.

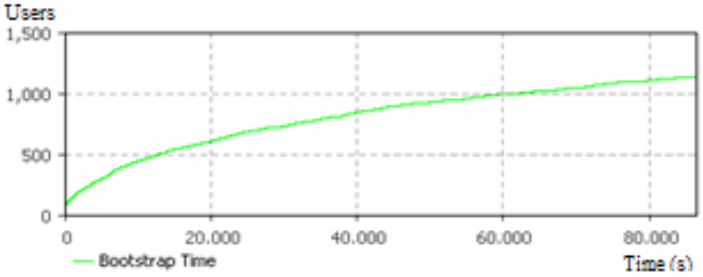

Fig. 5. Bootstrap time with 20,000,000 system users worldwide.

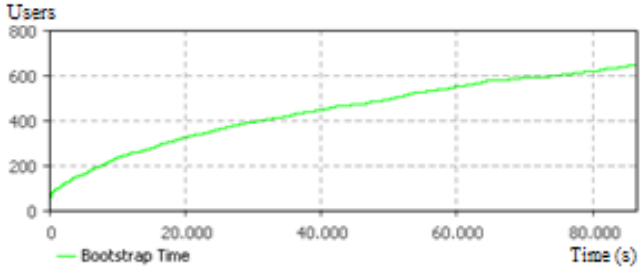

Fig. 6. Bootstrap time with 2,000,000 system users worldwide.

As can be seen from the results, if we want to achieve the aforementioned objective of half the agents having shared their Wi-Fi with foreigners in a reasonable time, the only configuration achieving this is the one with 200 million system users. This accounts for 750 agents in roughly 7,500 to 8,000 seconds, which is close to the average time for agent renewal in the simulation, making it a feasible time for the system to be bootstrapped.

Resource Depletion Measurements

Another interesting measurement for us is how quick users run out of data capacity, and which is the average time that it takes for a given user to be depleted of her data capacity.

We have run the simulation for different sizes of user base population, ranging from 2 million system users to 200 million system users with an intermediate simulation accounting for a 20 million system user base. For each of the figures, the left-hand graph represents the amount of data depleted users in a given point of time, being the Y axis the amount of users and the X axis the time in seconds, and the right-hand graph represents the average time that took for those users to be depleted of their data capacity, measured in seconds. The results can be seen in Figs. 7-9.

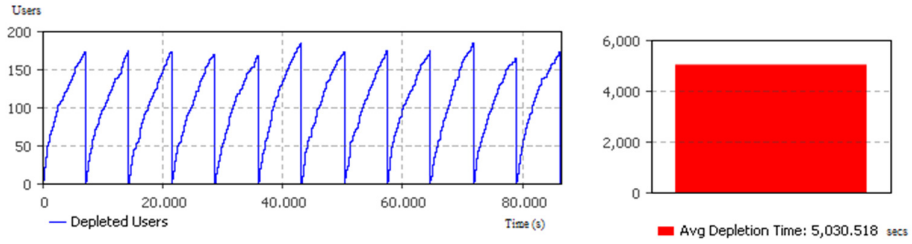

Fig. 7. Amount of depleted users and average depletion time with 200,000,000 system users worldwide.

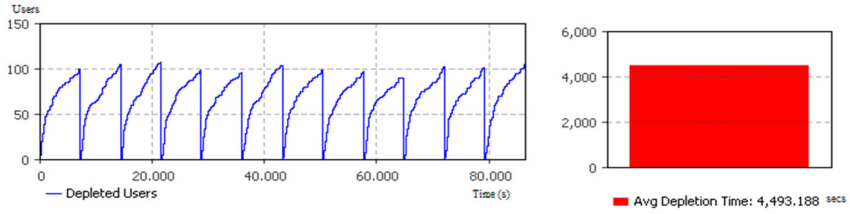

Fig. 8. Amount of depleted users and average depletion time with 20,000,000 system users worldwide.

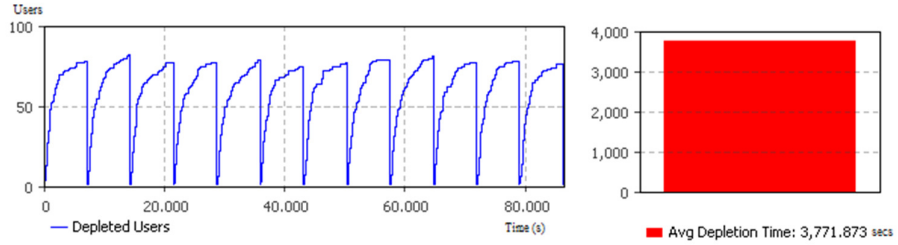

Fig. 9. Amount of depleted users and average depletion time with 2,000,000 system users worldwide.

As can be seen from the results, with a smaller system user base the amount of depleted users in each renewal period is also smaller, but the average depletion time for each of those agents is lower as well. The implications of this will be discussed in the next subsection.

5.3 Discussion

From the previous simulation runs carried out, we can summarize the results in Table 2 as follows:

Table 2. Summary of results

User Base (in millions)	Bootstrap time (in hours)	Depleted users per renewal period	Average depletion time (in hours)
200	2.26	175-185	1.39
20	7.87	95-105	1.24
2	> 24	75-85	1.04

As can be seen from the summary in Table 2, the bigger the system user base is, the better the results, both in terms of bootstrapping time and depletion measurements.

Regarding bootstrapping results, with a bigger user base it is more probable to find a chain connecting a service requester with a service provider, accounting for the shorter bootstrapping time, as it is more likely to find users who can transfer some trust points from one end to the other and thus enabling cooperation in between the two users. It is also worth to note that with the use of the system the probabilities of finding users from which to get points increases as the interactions in between agents increase. This translates into an increase of the probabilities of finding a chain of agents from which to get points lent from one end to the other by 0.1% per interaction per agent. Arguably, it could be said that a 20 million user base could be enough to obtain a reasonable bootstrapping time (~7.8 hours), but with a user base closer to 200 million we can achieve times which are closer to the agent renewal time in our scenario, making it closer to the ideal situation.

Regarding data depletion, as true as it is that with smaller system user amounts there are less agents that get depleted from their daily quota allowance, this is due to the fact that also there are less agents being able to connect and to allow connections in order to share Wi-Fi as it is more difficult to find a longer user chain to transfer trust points. In the other hand, it can also be seen that the average time taken to deplete a user from her daily data quota is higher the bigger the user base is, meaning that even though more users are depleted in each agent renewal period, those users take longer to be depleted due to the higher amount of agents being able to share their Wi-Fi connection. It is also worth to note that even being a higher number of depleted users, those account only for ~10% approximately of the total amount of agents being able to share their Wi-Fi connectivity (175-185 out of 1500).

6 Conclusion and Future Work

In this paper, we have proposed extending trust management with cooperation incentives for collaborative Wi-Fi sharing and we have identified the most important shortcomings affecting these kinds of services and systems. Through the use of trust management and cooperation incentives we have put in place measures to eradicate or mitigate all of them, and finally, we have shown through simulation the effectiveness of the combination of our trust and cooperation incentives schema in regards of bootstrapping time and data depletion, linking it to the amount of users the system has and finding which is that ideal amount.

It is left for future work to compare our trust metric and incentives schema with other trust metrics such as EigenTrust or Appleseed.

Acknowledgments

The research leading to these results has received funding from the EU IST Seventh Framework Programme (FP7) under grant agreement n° 318508, project MUSES (Multiplatform Usable Endpoint Security), grant agreement n° 257418, project ULOOP (User-centric Wireless Local Loop) and grant agreement n° 258142, project TEFIS (TEstbed for Future Internet Services).

References

1. International Telecommunication Union (ITU) report, “The World in 2013: ICT Facts and Figures”, 2013.
2. Agustín Díaz-Pinés, “International Mobile Data Roaming”, Organization for Economic Co-operation and Development, May 2011.
3. Garrett Hardin, "The Tragedy of the Commons," Science #13, pages 1243-1248, December 1968.
4. Gian Maria Greco and Luciano Floridi, “The Tragedy of the Digital Commons”, IEG - Research Report, October 2003.
5. C. Macian and J. Infante, “The tragedy of the commons vs. P2P success: An analysis of the conditions for cooperative sustainability in the file-sharing world”, ITS 2008, Montreal, Canada, June 2008.
6. Aldini, Alessandro, and Alessandro Bogliolo. "Model Checking of Trust-Based User-Centric Cooperative Networks.” AFIN 2012, Rome, Italy.
7. Fernandes, A. et al. Pinocchio: Incentives for honest participation in distributed trust management. In Trust Management (pp. 63-77). 2004. Springer Berlin Heidelberg.
8. Open Garden, http://opengarden.com/
9. ULOOP Project, http://www.uloop.eu
10. Air Mobs, http://eeiiaa.com/blog/?p=785
11. Milgram, Stanley. "The small world problem." Psychology today 2.1 (1967): 60-67.
12. Backstrom, Lars, et al. "Four degrees of separation." Proceedings of the 3rd Annual ACM Web Science Conference. ACM, 2012.
13. Ugander, Johan, et al. "The anatomy of the facebook social graph." arXiv preprint arXiv:1111.4503 (2011).
14. Klemm, Konstantin, and Victor M. Eguiluz. "Highly clustered scale-free networks." Physical Review E 65.3 (2002): 036123.
15. Crucitti, Paolo, et al. "Efficiency of scale-free networks: error and attack tolerance." Physica A: Statistical Mechanics and its Applications 320 (2003): 622-642.
16. Geneva Airport Statistics, http://gva.ch/en/desktopdefault.aspx/tabid-244/.
17. Seigneur, Jean-Marc, Alan Gray, and Christian Damsgaard Jensen. "Trust transfer: Encouraging self-recommendations without sybil attack." *Trust Management*. Springer Berlin Heidelberg, 2005. 321-337.
18. AnyLogic simulation framework, http://www.anylogic.com/.