COOPERATIVE WI-FI-SHARING: ENCOURAGING FAIR PLAY

Hanno Wirtz, René Hummen, Nicolai Viol, Tobias Heer, Mónica Alejandra Lora Girón and Klaus Wehrle

Chair of Communication and Distributed Systems
RWTH Aachen University
{wirtz, hummen, viol, heer, lora, wehrle}@cs.rwth-aachen.de

ABSTRACT

Cooperation enables single devices or applications to establish systems that exceed the capabilities of single entities. A prime example for cooperation are Wi-Fi-sharing networks, in which multiple parties cooperatively share their resources, such as wireless access points and Internet uplinks, to form a large-scale Wi-Fi network that offers access to mobile users. Mobile users benefit from this network by gaining free network access at every access point of the network. However, such cooperation needs to be established in the first place by providing incentives to users to join the network. Furthermore, in an established network, users need incentives to behave cooperatively when using the network. Frameworks to provide incentives and to regulate user behavior in the presence of malicious parties can exist at multiple levels: The technical level inside the given network, a contractual level that regulates the operation of the network and the legislative level that establishes general rules for the operation of Wi-Fi-sharing networks. In this paper, we analyze requirements and mechanisms to establish such frameworks at each level and discuss possible solutions and existing examples.

Index Terms— Cooperative networking, Ubiquitous networking, Wi-Fi-sharing

1. INTRODUCTION

Cooperation is a compelling concept to surpass the technical and conceptual restrictions of a single device or application. It can enable the creation of new networks and services that a single user or device could not establish by itself. Building on this notion, cooperation is a fundamental principle at different levels in many of today's network approaches. For example, message forwarding and data aggregation in multi-hop wireless networks such as wireless mesh or sensor networks are built entirely on the principle of cooperation between the participating nodes. Peer-to-peer (P2P) networks, on the other hand, use cooperation not between system entities but between users at the application level. The benefits of cooperation in these scenarios include the establishment of communication beyond the communication range of an individual radio and access to otherwise unavailable resources, such as storage space and information.

As in other systems comprised of strangers, cooperative users are tempted to defect, i.e. to behave selfishly and follow their own interests. As a result, their behavior may stand in stark contrast to the interests of the other cooperating parties and may degrade the overall cooperative system. In addition, evolution theory has shown that, cooperation cannot sustain without any support through regulations [1]. The prime example for defective behavior in P2P networks is "Free-riding", where users exploit the resources of the network without providing resources back to the network. Still, users need to show preliminary trust when providing a service without a guarantee for benign behavior of other users, in order to enable an initial network creation. In the further course of network operation, mechanisms are required for users to check whether this initial investment of trust is justified by the cooperative behavior of other users. In consequence, the risk of defecting users requires *incentives* for individuals to cooperate and a framework that allows to detect defection. In case a user shows *defective behavior* in the network, e.g. stops cooperating, or misuses a given resource, such a framework establishes rules for penalizing or excluding defecting users.

In this paper, we analyze Wi-Fi-sharing networks as a case study for the implementation of different aspects of cooperation. Cooperative Wi-Fi-sharing networks and their services rely on the contribution of Wi-Fi resources and Internet uplinks by participating users. However, the operation of such networks also affects external parties such as Internet Service Providers (ISPs) that operate the wired uplink for the shared wireless network. Hence, analyzing Wi-Fi-sharing networks with regard to cooperation requires to look at mechanisms for a regulatory framework of cooperation at multiple levels. We identify three hierarchical levels, as shown in Figure 1, on which frameworks for user cooperation can be established: i) the technical level, ii) the contractual level, iii) and the legislative level. As Wi-Fi-sharing networks account for the interests of the different participating parties as well as the respective judicial framework, single networks typically differ on the technical and contractual level. As such, no standardized scheme for Wi-Fi-sharing networks exists as

This work is supported by the Ziel2.NRW program and the ERDF fund of the European Union.

of now. A push towards standardized Wi-Fi-sharing could be provided by ISPs that propose network modes and technical mechanisms for standardization. Standardized frameworks and mechanisms would provide additional support for the acceptance and interoperability of Wi-Fi-sharing networks.

Figure 1 illustrates the scope of the respective frameworks on each level as well as the diversity of frameworks. The *technical level* enables monitoring and controlling of user behavior based on network-centric mechanisms. The choice of specific mechanisms to be implemented depends on the agreements at the contractual and legislative level. The *contractual level* predominantly enables agreements between the parties participating in a cooperative Wi-Fi-sharing network. Defecting users of a network that are identified by technical means can then be punished or excluded based on contractual agreements within the specific network. The *legislative level*, on the other hand, governs regulation in a network-independent way. Laws passed by the legislative power form the standardized basis for the relationship between participants of the Wi-Fi-sharing network and external parties. This hierarchy allows the top-down definition of rules and the subsequent control and punishment of participant behavior in cooperative Wi-Fi-sharing networks in a bottom-up fashion.

The remainder of this paper is structured as follows: In Section 2, we introduce the concepts of cooperative Wi-Fi-sharing networks and the affected parties in this specific network scenario. Section 3 gives an overview over technical agreements and presents cooperation strategies and actual implementations. Furthermore, we discuss quality metrics and measures supporting user incentives. We focus on the community scope and the effect of contracts and agreements within a network in Section 4. Section 5 discusses the role of legislation and shows how laws regulate user behavior on a nation-wide scope with respect to cooperation. Finally, we conclude this paper and present an outlook on cooperative Wi-Fi networks in Section 6.

2. WI-FI-SHARING NETWORKS AND COOPERATION

The availability of cheap wireless router hardware and a free wireless frequency band have created numerous user-driven initiatives to create cooperative networks as a cost-efficient alternative to provider-driven Wi-Fi networks. Examples for such Wi-Fi-sharing networks are the Freifunk [2] and Funkfeuer [3] initiatives in Berlin and Vienna, respectively, as well as the roofnet project in Cambridge [4, 5] and its spinoff Meraki [6]. The fundamental principle of these networks is cooperation by means of resource sharing. Participants of the Wi-Fi-sharing network provide network access to other participants as *micro operators* at their own AP while in turn receiving wireless access at other residential APs when they are mobile. At the technical level, Wi-Fi-sharing networks often build on existing standards such as the IEEE 802.11 infrastructure or ad-hoc mode. However, additional proprietary mechanisms may be added at the link layer and above according to the provider's or the community's design. Likewise, the terms and conditions of the network typically differ between networks depending on their respective provider model. As such, each Wi-Fi-sharing network establishes its own set of *internal standards* on the technical and contractual level that only apply to this very network. Lastly, the different legislative frameworks in different countries hinder a global standardization of how Wi-Fi-sharing networks can be realized.

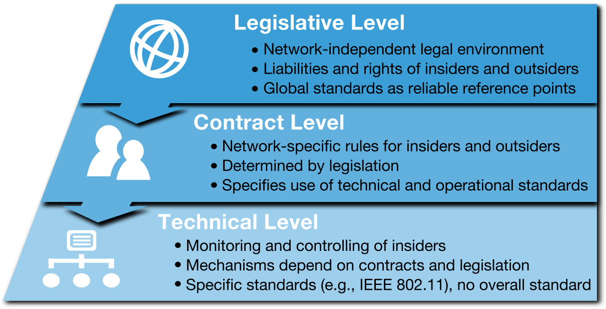
Legislative Level
• Network-independent legal environment
• Liabilities and rights of insiders and outsiders
• Global standards as reliable reference points
Contract Level
• Network-specific rules for insiders and outsiders
• Determined by legislation
• Specifies use of technical and operational standards
Technical Level
• Monitoring and controlling of insiders
• Mechanisms depend on contracts and legislation
• Specific standards (e.g., IEEE 802.11), no overall standard

Fig. 1. Frameworks to regulate user behavior and define network operation on different hierarchical levels.

Due to the ongoing interest in these cooperative Wi-Fi-sharing networks, their network size has in many cases exceeded a level on which trust relations between every pair of users are possible. To handle such networks, a legal basis, in the form of a pico peering agreement [7], has been established to regulate the service provision by micro operators. This agreement states that users provide free data transit and open access while including a liability exclusion for the micro operator. However, while this agreement defines the legal aspects of service provision, corresponding technical measures to enforce proper user behavior and to detect misbehavior in such open networks must be provided.

Building on community concepts, companies such as FON [8] and Wippies [9] offer *commercial Wi-Fi-sharing products*. These companies offer customized IEEE 802.11 access points (APs) to community members in order for them to give access to their residential broadband connection. However, provider-driven Wi-Fi networks not only allow access for community members, but typically offer additional tariffs at which non-members can rent access to the network. These tariffs can either be time- or volume-based; the resource usage thus has to be measured by trustworthy, standardized tools to avoid disputes over fairness or fraud. Network providers thus become a stakeholder in the network and have to ensure that legal aspects and user contracts are fulfilled within the cooperative network.

Finally, a number of Wi-Fi-sharing networks exist as ongoing research-driven design concepts or architectural prototypes. Mobile ACcess [10] is an example for such a concept.

It enables multiple parties such as private users, companies, universities, and municipalities to provide a unified cooperative network at company APs, on campus, or in public places. It has similar properties as commercial Wi-Fi-sharing networks, but does not depend on the presence of a single central network provider. In previous work, we introduced a general framework for securely providing such a network by means of PISA [11] and PISA-SA [12] and discussed challenges and applications for municipal Wi-Fi-sharing networks in [13]. In this paper, we focus on the aspects of cooperation within the scope of Wi-Fi-sharing networks and the parties affected by such networks.

2.1. Parties Affected by Wi-Fi-Sharing Networks

Insiders of the Wi-Fi-sharing network are users that provide broadband network access as well as network providers in commercial settings. In the network, insiders act out of their respective interests. However, as individual interests might interfere with the interests of the cooperative system, a balance between the strive for maximal personal gain and a fair use of the network needs to be ensured. As actions and repercussions of insiders occur in and affect the Wi-Fi-sharing network at hand, a regulation of insider actions is therefore achieved best on a per-network level. This then allows to enforce insider behavior by means of technical mechanisms within the network and membership contracts.

ISPs and other parties that are affected by but do not directly take part in the network can be considered as *outsiders* of a cooperative Wi-Fi-sharing network. ISPs only implicitly become stakeholders in the network as residential user Internet uplinks are provided by them. Hence, ISPs are providers of the backbone of a cooperative network, possibly even without being aware of this fact. Thus, explicit regulations are required between the ISP and the user as well as between the two economic entities, the ISP and an eventual provider of the Wi-Fi-sharing network. These regulations have to regulate insider behavior to not harm possibly unknowing outsiders and need to clarify the position of outsiders with regard to insider behavior.

3. TECHNICAL AGREEMENTS

Wi-Fi-sharing communities rely on cooperation on the network level. To balance the contribution and consumption of shared resources between community members, they must adhere to a common set of rules and conventions. If these conventions are not met, some members provide far more than they receive, others may be subject to malicious actions of others. As a first rule, users that expect other users to provide wireless Internet access need to open their own access point to other community members. Second, users should use the provided Internet access respectfully and within the bounds of the law because otherwise the access point owner may appear as the originator of the illegitimate action. Both of these rules are difficult to enforce because illegitimate user actions cannot be foreseen and may only prove illicit or selfish in hindsight.

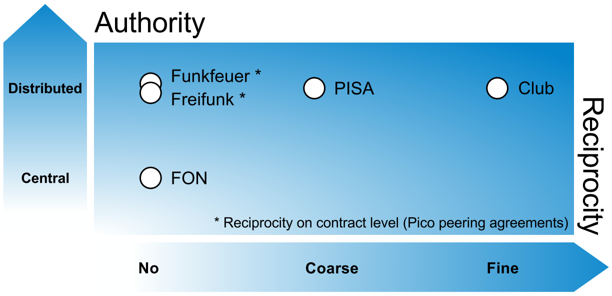

Fig. 2. Use of reciprocity schemes and distribution of authority in different cooperative Wi-Fi-sharing systems.

Since no a-priori trust and no proof of legitimacy between users exist, an initial investment of trust is needed to bootstrap the system. However, users need to be able to check whether their trust in other users is justified. In this section, we discuss incentives and mechanisms to motivate, check and enforce user behavior with regard to both aspects mentioned above. We focus on the concepts of these mechanisms as their actual implementation is network-dependent.

3.1. Incentives to Contribute

The most powerful incentive for a user to contribute is a personal benefit that outweighs his invested resources. Hence, in a balanced system, each user experiences a personal gain or payoff from cooperating. The assumption that the other users will provide this gain is the basis for an initial cooperation. Consequently, if cooperation fails and the payoff decreases, this assumption proves unjustified and the trust in the cooperation of other users diminishes. In such a situation, the lacking of trust will cause discontinuation of the cooperation.

Reciprocity, the act of rewarding a positive action with another positive action, explicitly encourages cooperation and discourages defective behavior as cooperating users directly experience personal benefits. Fitzek et al. compare different cooperation strategies [14]. They show that reciprocal strategies prove more lucrative than non-reciprocal strategies in the long run, although pure defective behavior appears more profitable in the first place. Hence, in cooperative Wi-Fi-sharing networks, reciprocity schemes foster the trust in cooperation and the mutual interest in providing Wi-Fi resources and Internet uplinks.

On a technical level, initial trust can be rewarded through reciprocity in three ways: i) Through the implementation of a coarse-grained reciprocity scheme that allows for personal payoffs but lacks mechanisms to adapt to differences in resource provision or consumption, ii) by operating a fine-grained reciprocity scheme that allows for rewarding resource provision to other users with providing the same amount of this resource back to the user at foreign APs and iii) by incorporating multiple aspects of quality of the provided services as a metric to further differentiate between the contribution to the network made by different users. Figure 2 shows different actual networks and the implemented type of reciprocity scheme in this network. In the following, we discuss each of these technical concepts for achieving reciprocity as the basis for sustainable cooperation in a network.

3.1.1. Coarse-Grained Reciprocity

In a cooperative Wi-Fi-sharing network, the most basic form of participation is the provision of a user's Wi-Fi connectivity and Internet uplink to other users. This in turn is the requirement for the basic reward for this user, namely network access at APs provided by other users. Thus, rewarding the user with network access in a coarse-grained reciprocity scheme, requires him to provide network access at his own AP. However, single users do not directly interact with other users but rather perceive the cooperative Wi-Fi-sharing network as one single network [13]. Each user thus interacts with the whole network, in case a user does not share his AP or stops providing network access, access at all other APs, i.e. access to the whole network, will be denied.

A coarse-grained reciprocity scheme thus implements a basic access control mechanism in the Wi-Fi-sharing network. This mechanism requires a means of checking if users cooperate. The result of this check is then used to determine whether or not a user may gain access to the network. We discuss two different ways of implementing such a means: a) login-based access control with a central access control server as implemented by FON and b) decentralized certificate-based access control as proposed by PISA.

The FON network [8] requires the user to log in to a webpage once he wants to access the network. Upon login, the network checks whether the AP that is associated with this user is online and thus providing network access to other users. In case the user does no longer cooperate with the network, i.e. if the user's AP has been offline for a prolonged time, network access is denied. As the status of user cooperation is defined, checked and enforced by a central online authority, the mechanism used by FON is an example for a centralized scheme of ensuring reciprocity.

In PISA [11], no such online central entity exists. Rather than identifying a user by his username and password, PISA employs standardized cryptographic certificates, such as SPKI or X.509 certifcates, to express network membership and to identify specific users. Once a mobile user requests access at a foreign AP, the AP checks the provided certificate for validity and only forwards any subsequent traffic if the certificate is valid. Certificates are periodically renewed, with the criteria for renewal being the ongoing cooperation by the user in providing his AP to the network. In PISA, AP availability is implicitly checked as all Internet traffic is routed through the mobile user's own AP. In case this redirection fails, the current AP may stop providing network access to the mobile user. Similar to FON, the certificate is revoked if the user stops cooperating.

As shown in Figure 2, a coarse-grained reciprocity scheme can be implemented in a cooperative Wi-Fi-sharing network using these mechanism. While PISA also distributes the authority for user exclusion among all network entities, FON employs a single central entity. However, a user may provide only a fraction of his resources and still get high-quality network access across the network. To account for the actual contribution to the network in measures such as traffic volume or AP uptime, a more fine-grained reciprocity scheme is required.

3.1.2. Fine-Grained Reciprocity

The problem of unfair resource consumption in a cooperative Wi-Fi-sharing network arises in different forms. First, a user might only make a fraction of the total bandwidth available to other users using traffic-shaping techniques at his AP. When using other users' APs, however, he might fully exploit the available bandwidth, thus creating a significant imbalance between the resources he offers and the resources he consumes. Second, a user whose AP is located in an unfrequented area might experience little resource consumption because few users use his AP. As this user might access and use the network in more frequented places, the balance of the system suffers.

A suitable parameter to measure and return a user's contribution in a Wi-Fi-sharing network would be the amount of network traffic that has been provided to others. In [15], Efstathiou et al. describe such a mechanism for community Wi-Fi-sharing networks. In this approach, users that generate traffic at a foreign AP issue a *receipt* for the time they use the AP and the amount of traffic they generate at the foreign host AP. These receipts are cryptographically secured and also denote the pair of users that exchanged resources. When using the APs of other users, the AP owner uses these receipts to receive access to the network as he can prove his cooperation and the amount of resources he offered.

This approach solves both of the above mentioned problems. First, users that offer only little bandwidth will in turn be able to request only little bandwidth in the network as the receipt clearly states the provided amount. Second, users that are not able to generate enough receipts may form groups, for example with friends that own well-frequented APs, and distribute the accumulated receipts of that group among its members. The *Club* network proposed by Efstathiou et al. implements this approach, as shown in Figure 2. However, this approach favors users that provide APs in well-frequented places as forming a group to collectively gather receipts may slow down the acceptance of the system in less well-frequented areas. Furthermore, to avoid disputes over the measured and provided amount of resources, standardized tools need to be used to carry out these measurements. Similar to the case in provider-driven networks, tools that are approved by an external organization or globally standardized support the trust of users in the operation of the measuring system and the overall network.

While this approach mainly considers the consumed traffic volume, a metric that combines multiple factors may give a more detailed measure of user contribution. We discuss such multi-dimensional schemes in the next section.

3.1.3. Fine-grained Quality-based Strategies

Single-dimensional metrics, such as the provided traffic volume, can neither express the combined *Quality of Service* (QoS) provided by a user nor the other users' *Quality of Experience* (QoE) when using the AP of other users. For example, a highly frequented AP may provide a large traffic volume even though the bandwidth at this AP is artificially limited or a transmissions cannot be received by clients due to packet collisions. Combining synthetic QoS parameters with user-provided QoE feedback, however, would allow for an overall evaluation of user cooperation.

To derive the QoS of a service, standardized methods [16] and frameworks [17] are available. The estimation of a specific QoS then includes synthetic parameters that can be measured at both the AP and the client, such as delay, bit rate, packet loss and jitter. Furthermore, the ITU Recommendation G.1000 [17] includes customer requirements, QoS offered by the provider and the achieved QoS as parameters. Following these recommendations, the AP and the client can derive a consensus value of the achieved or measured QoS and issue receipt-like structures as in [15]. Using these receipts to gain access at other APs, a consistent, network-wide QoS-based strategy can be used to recompense user contribution.

Building on QoS measurements as a technical basis, QoE measurements could augment this basis by user-provided feedback. These measurements should reflect perception, context and expectations of the user with regard to the services and system performance of the Wi-Fi-sharing network [18]. In a QoE-based scheme, the user is thus required to rate the current service in periodic time slots to establish a measure of the overall quality and usability of the network access provided by this AP. However, there are no standardized approaches for assessing QoE yet. Hence, providing a consistent metric based on user experience is difficult. QoE standardization activities in ITU-T Study Group 12 (SG12) are ongoing [19], nevertheless the scope of many of the current questions would need to be extended to establish multidimensional QoE assessments in Wi-Fi-sharing networks.

A significant problem assessing user cooperation through QoE ratings is the number of possible reasons for a bad user experience. For example, a slow downlink may be caused by traffic shaping at the AP, indicating defective behavior, or simply by the user being located far away from the access point. Making a distinction between these cases is not possible for the end-user. Hence, purely observing QoE as a metric for cooperation may be far-fetched and can prove error-prone. We are not aware of a cooperative Wi-Fi-sharing network that thoroughly incorporates QoE or QoS metrics in its reciprocity scheme. Standardized tools such as the ITU Recommendation G.1000 framework, could provide a basis for mechanisms that incorporate quality-based metrics for user contribution.

Next to user contribution, *user behavior* in the cooperative Wi-Fi-sharing network needs to be monitored and regulated. We discuss frameworks and approaches to mitigating or preventing malicious user behavior in the following section.

3.2. Incentives to Behave

Typically, users behave well in their own home networks since they use the Internet connection they pay and are liable for. In contrast, the use of Internet connectivity at community members' access points may tempt users to misuse these shared resources because of a missing perception of responsibility and liability [20]. Possible misuses range from overuse of the shared resources to committing Internet fraud. Hence, if malicious user behavior is expected, mechanisms must be established within the network to identify and eventually penalize misbehaving users, e.g., by revoking their access rights to the network.

Technical and legal actions against misbehaving users are only possible if their behavior can be observed and documented. Thus, *non-repudiation* is a basic requirement to successfully deal with misbehaving users. In this regard, network traffic generated within the cooperative Wi-Fi-sharing network needs to be clearly traceable and attributable to a specific device or user. In the following sections, we show two approaches of implementing the authority in the network to achieving this attribution, namely *centralized* authentication and logging structures and *decentralized* control mechanisms. We illustrate the use of these approaches in different Wi-Fi-sharing networks, as shown in Figure 2.

3.2.1. Centralized Approach

In a centralized approach, a single entity in the network, the network provider, takes over responsibility to control user behavior and to eventually penalize misbehaving users. We identify two options for the network provider to exercise its control at the technical level: *traffic-based* control and *service-based* control.

For traffic-based control, the network provider requires users to log in before using the network at another member's access point and centrally logs Internet traffic and transaction data generated by the user. The network provider maintains

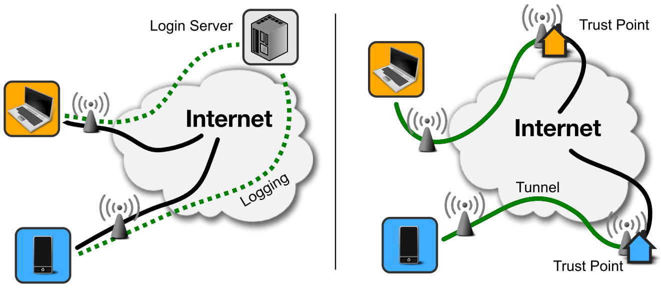

Fig. 3. Centralized logging (left) as used in FON and decentralized tunnel approach (right) as introduced in PISA.

a history of past user logins in combination with the stored traffic information. This logged information enables the network provider to identify the original user in case of misuse of network resources. A real-world example of a centralized log-based approach using a single login server is FON, as illustrated in Figure 3. While no actual traffic traverses the login server, it is contacted in each connection attempt by a mobile user. The general logging mechanism resembles the technique ISPs are forced to implement under the data retention act [21] in Germany and the EU. In addition, Wi-Fi-sharing networks that route all traffic from the cooperative network through a central backbone use logging techniques that equal the logging of a wired ISP.

A basic requirement of this log-based incident handling is that the network provider is a trustworthy entity because otherwise it cannot prove the responsibility of a user in a law suit. Hence, this approach is only possible if the logging is performed by an ISP-like trusted entity. Provider-less Wi-Fi-sharing networks without dedicated central entities (e.g., Freifunk and Funkfeuer) cannot use logging as the basic mechanism because it leaves users with their word against the word of other users in a law suit. Here, the question which user is more trustworthy (the user that logged the actions or the user that presumably acted inappropriately) is difficult to assess.

With service-based control, on the other hand, a network provider limits network access to a restricted set of services. While this does not enable the provider to identify the traffic originating user, it allows control over which content is accessible in the network. If the network provider ensures that no illegal information is accessible within the set of provided services, this renders traffic-based control mechanisms unnecessary. Restricted services are typically offered to unregistered clients at commercial hotspots as the main incentive to gain new users.

One important aspect common to both options is the requirement for the network provider to exercise control over the hardware and software used in the deployed user APs. Otherwise, malicious users can easily bypass the mechanisms used on the APs enabling enforcement of user behavior on both the traffic and service level.

3.2.2. *Decentralized Approach*

A fully decentralized cooperative Wi-Fi-sharing network does not provide a central point in the network where user control and penalties can be implemented. Likewise, mechanisms such as distributed logging of traffic information at individual APs do not suffice as a malicious user may provide false control information, i.e. traffic logs, about other users. Instead, decentralized networks need to mitigate the incentive for a user to misbehave at an architectural level.

In PISA [11], as an example for a decentralized cooperative Wi-Fi-sharing network, we remove the motivation for a user to misbehave at another member's AP. We achieve this by redirecting all Internet traffic over a secure tunnel to the home network of the mobile user. The home network then forwards the traffic to the original destination in the Internet. Figure 3 illustrates the flow of traffic from the mobile user to the Internet. This effectively makes the user's home network appear as the egress point of all traffic generated by the user – a situation comparable to when the user accesses the Internet from within his home network. Hence, this approach encourages benign user behavior by ensuring direct legal liability for the traffic the user generates at other members' APs. Furthermore, only legitimate devices can connect to the user's home network by pairing user devices with the user's home network in an initial step and by performing subsequent mutual authentication between the end-points during the establishment of the secure tunnels. This prevents outsiders and malicious insiders to exploit the secure tunnel mechanism.

While the actual use of the network occurs on the technical level, a network-specific framework for this use is necessary. This framework is based on standards such as IEEE 802.11 for communication and SSL for security and regulates the relations and rights of participants in the network. Furthermore, the general operation of this network with respect to the economic interests of insiders and outsiders needs to be defined. We discuss the contractual means of regulating both in-network operation as well as economic regulation of Wi-Fi-sharing networks in the next section.

4. COOPERATION BY CONTRACT

Technical agreements and implementations directly establish and regulate the use and user behavior inside of the network. However, this set of fine-grained rules needs to be embedded in a contractual framework that defines the more general network aspects. Examples for such higher-level rules are the definition of security standards that are required for communicating in the network or agreements about the rights and duties of users. Rules that are defined in contracts may thereby i) define a framework for benevolent actions in a cooperation, ii) define a framework for network-wide consequences of malicious actions and iii) define the obligations of a network user and his role in the network. As a best practice, these rules should rely on technical standards and software wherever possible to ensure an easy acceptance and a lasting contribution. Above all else, contracts serve as a fixed point of reference which allows for an assessment of actions in the network and defines eventual consequences.

There are numerous examples for contracts in cooperative networks. *Pico peering agreements* [7] as used in Wi-Fi-sharing communities such as FON [8], e.g., regulate which services cooperating users have to provide as participants of the network. Such a contractual definition is necessary to check if access point owners are behaving correctly. The sustained operation of Wi-Fi-sharing networks directly depends on such checks to prevent misuse of the network and defection of benign users that put trust into other participants when they joined. Also, these checks form the basis for exclusion of defecting AP owners.

Next to network regulation, contracts also form a basis of cooperation between the network provider and ISPs to satisfy the economic interests of both parties. First, a contract may define the monetary arrangements between the network provider and the ISP and defines a set of rules that allows the ISP to sue in case of illegal actions of the network provider or users. Second, payments and subscription fees for users of the network are determined by contracts prior to network operation. Certain conditions may thereby require technical mechanisms to be realized. For example, network access for a user who bought a day pass for a commercial Wi-Fi-sharing network needs to be technically revoked after the day pass has expired.

Contracts thus serve as a single-network framework regulating user behavior and economic interaction. On a broader scope, a similar framework is needed to govern the fundamental rules and regulations concerning the establishment, operation and limits of Wi-Fi-sharing networks. As this exceeds the scope of a specific network but rather applies to every such network, applicable laws that provide a legal framework for Wi-Fi-sharing networks are required.

5. THE IMPACT OF LEGISLATION ON COOPERATIVE NETWORKS

The legislative power defines the legal framework that provides the operational context for Wi-Fi-sharing networks in general at the national level. To do so both on a legal and contractual level but also with regard to approved technical means, laws in this context depend on standards as a basis and as orientation points. In case actions by insiders or outsiders violate these laws, enforcement of the appropriate consequences or exclusion from the network can be achieved through judicial power. Legislation may thus provide the basic rules of conduct for cooperation in two different ways: first by definition of the legal environment and second by protection of interests of insiders and outsiders.

One example for a definition of the environment in which cooperation takes place are laws that define the liabilities of the involved parties. In this sense, the regional court of Mannheim, as a representative of the judicial branch in Germany, decided in 2006 [22] that owners of Wi-Fi access points are partially liable for any Internet traffic generated from within their local network. The decision was based on existing legislation, where the defendant has to prove his innocence (§138 Abs. 2 ZPO), and was recently confirmed by a verdict at the German Federal Court in 2010 [23]. Hence, in Wi-Fi-sharing, the AP owner is responsible for any traffic generated by other users at the shared AP. Such regulations have a significant impact on the design and operation of a Wi-Fi-sharing network and thus on the incentives for a user to join and participate. While such decisions and laws in general do not directly set or mandate standards with regard to Wi-Fi-sharing, they refer to current standards and mandate the use, e.g., of well-established security standards to protect the local wireless network [23].

The legislation may also protect the business interests of insiders and outsiders, an example for which is the decision made at the regional court of Cologne in 2009 [24]. Here the verdict explicitly forbids providers of a Wi-Fi-sharing community to rent out Wi-Fi-based network access at private homes to (non-)community members, as these use the Internet uplinks of third-party ISPs. The decision is based on recent competition regulations in Germany. Regulations such as this one impose restrictions on how cooperative network operation may affect parties outside of the network.

However, legislative mechanisms typically have a very broad scope and do not provide rules for specific cooperative network scenarios such as for distinct Wi-Fi-sharing networks. If rules are required on a more fine-grained network- or location-specific level, contracts and technical measures are used based on individual terms and conditions for a network.

6. CONCLUSION

In this paper, we analyzed cooperative Wi-Fi-sharing networks as a prime example of cooperation on different levels. Cooperation happens on the technical level inside of a given network, the contractual level that defines the general network operation and the legislative level on which the general rules for Wi-Fi-sharing networks are established. While cooperation benefits all participating parties, selfish and defective behavior needs to be accounted for. Based on this notion, we discussed incentives and frameworks to motivate and regulate user behavior on each level with the goal of providing the maximum benefit for each user while achieving a sustainable network operation.

At the technical level, we discussed possibilities of supporting cooperative behaviors of users and frameworks that allow for checking user behavior and eventually penalizing malicious user actions. The contractual level establishes the general rule of operation in which implementations on the technical level need to be realized. Furthermore, the economic interests of parties acting inside of the network and parties outside of it, such as ISPs, are regulated on this level. On the legislative level, the economic interests of outsiders in competition are regulated and fundamental laws regarding the legal liability of insiders and outsiders are given. Traversing these three levels from the bottom up, the scope of rules widens from a per-network scope to a country- or continent-wide scope, such as in Germany and the European Union, respectively.

We expect cooperative Wi-Fi-sharing networks to gather continuous interest as a cost-efficient way to provide Internet access to mobile users. However, we assume their scope to be local, i.e. city-wide, with high bandwidth connections and specialized services and a cooperation between geographically close users. This is because techniques such as UMTS provide highly mobile, general purpose Internet access on a national scope. However, for cooperative Wi-Fi-sharing networks to establish a sustainable local operation, strong incentives for contributing to the network and for using the network in a benign fashion need to be provided. We discussed different reciprocity schemes for creating such incentives through coarse-grained and fine-grained mechanisms that closely couple users' benefits to their contribution in the network. Furthermore, we assume a stable legal foundation for the establishment and operation of cooperative Wi-Fi-sharing networks to be necessary to attract network providers, ISPs and private persons on the basis of clear regulations with regard to legal liabilities and economic interests. While we expect no standards specific to Wi-Fi-sharing due to the different stakeholders and the complexity of single networks, ongoing interest of ISPs and commercial providers could strengthen the case for standardized partial solutions or usage frameworks.

7. REFERENCES

[1] M.A. Nowak, "Five rules for the evolution of cooperation," *Science*, 2006.

[2] Freifunk Community, "Freifunk Website," [Online] Available http://start.freifunk.net/, last visited July 12th 2011.

[3] Funkfeuer Community, "Funkfeuer Free Net Website," [Online] Available at http://www.funkfeuer.at, last visited July 12th 2011.

[4] MIT Roofnet Project, "MIT Roofnet Website," [Online] Available at http://pdos.csail.mit.edu/roofnet/, last visited July 12th 2011.

[5] J. Bicket, D. Aguayo, S. Biswas, and R. Morris, "Architecture and evaluation of an unplanned 802.11b mesh network," in *Proceedings of the 11th annual international conference on Mobile computing and networking (MobiCom)*, 2005.

[6] Meraki Inc., "Meraki Website," [Online] Available at http://www.meraki.com, last visited July 12th 2011.

[7] Funkfeuer Community, "Pico Peering Agreement," [Online] Available at http://www.funkfeuer.at/PicoPeeringAgreement.59.0.html, last visited July 12th 2011.

[8] FON WIRELESS, Ltd, "FON Website," [Online] Available at http://www.fon.com/, last visited July 12th 2011.

[9] Saunalahti Group Oyj, "Wippies Website," [Online] Available at http://www.wippies.com, last visited July 12th 2011.

[10] Mobile ACcess Project, "Mobile ACcess Project Website," [Online] Available at http://www.mobile-access.org/, last visited July 12th 2011.

[11] T. Heer, S. Götz, E. Weingärtner, and K. Wehrle, "Secure Wi-Fi Sharing on Global Scales," in *Proceedings of 15th International Conference on Telecommunication (ICT)*, 2008.

[12] T. Heer, T. Jansen, R. Hummen, S. Götz, H. Wirtz, E. Weingärtner, and K. Wehrle, "PiSA-SA: Municipal Wi-Fi Based on Wi-Fi Sharing," in *Proceedings of 19th International Conference on Computer Communications and Networks (IC-CCN)*, 2010.

[13] T. Heer, R. Hummen, N. Viol, H. Wirtz, S. Götz, and K. Wehrle, "Collaborative Municipal Wi-Fi Networks - Challenges and Opportunities," in *Proceedings of IEEE PerCom Workshops (PWN)*, 2010.

[14] F.H.P. Fitzek and M.D. Katz, *Cooperation in wireless networks: principles and applications; real egoistic behavior is to cooperate!*, Springer Verlag, 2006.

[15] E.C. Efstathiou, P.A. Frangoudis, and G.C. Polyzos, "Controlled Wi-Fi Sharing in Cities: A Decentralized Approach Relying on Indirect Reciprocity," *IEEE Transactions on Mobile Computing*, 2010.

[16] "Framework and methodologies for the determination and application of qos parameters," ITU-T Recommendation E.802, feb 2007.

[17] "Communications quality of service: A framework and definitions," ITU-T Recommendation G.1000, nov 2001.

[18] "New definitions for inclusion in recommendation itu-t p.10/g.100," Recommendation ITU-T P.10/G.100 (2006) - Amendment 2, jul 2008.

[19] Alexander Raake and Sebastian Möller, "Recent multimedia qoe standardization activities in itu-t sg12," IEEE COMSOC MMTC E-letter - Special Issue on Quality of Experience issues in Media Delivery, aug 2011.

[20] Daithí Mac Síthigh, "Law in the last mile: Sharing internet access through wifi," SCRIPTed 355, march 2009.

[21] Deutscher Bundestag, "Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG," [Online] Available at http://dip.bundestag.de/btd/16/058/1605846.pdf, last visited July 12th 2011.

[22] Regional Court Mannheim, "7 O 76/06," 2006.

[23] German Federal Court, "I ZR 121/08," 2010.

[24] Regional Court Cologne, "6 U 223/08," 2009.