19

Reputation-based Service Management and Reward Mechanisms in Distributed Cooperative Personal Environments

Malohat Ibrohimovna[1], Sonia Heemstra de Groot[1,2], Vijay S. Rao[1], and Venkatesha Prasad[1]

[1]*IDelft University of Technology, The Netherlands;*
[2]*Twente Institute of Wireless and Mobile Communications*

Personal Network (PN) is a person-centric, distributed environment of a person's devices that provides access to personal resources and services regardless the location of the person. A Federation of Personal Networks (Fednet) is a group-oriented network of PNs. A Fednet is a pervasive and ubiquitous computing technology that enables the users to enjoy cooperation and promises exciting opportunities for different applications in various fields, such as education, healthcare, entertainment, business and emergency.

Since each PN is associated with a person, i.e., the PN owner, the cooperation of the PNs reflects the social behavior of the PN owners, and therefore a Fednet can be seen as a social network of PNs. Trust and reputation influence the real-world interactions; similarly, using reputation as a metric for interactions between PNs is an interesting topic. In this Chapter, we look at the Fednets from the 'social' angle and discuss how the Fednets can benefit from using reputation. We propose a reputation-based framework for Fednets and present ideas on applying reputation information for service management and reward mechanisms in Fednets to improve the quality of cooperation between the PNs.

D. Kou (ed.), Demo Book, 1–20.

19.1 Fednets: Federation of Personal Networks

Almost everyone today has one or more personal devices at use in daily work, entertainment, communication and social activities. Most of these devices also have networking capabilities. Examples of such personal devices are mobile phones, PDAs, digital cameras, handheld game consoles, laptops, desktops, personal navigation systems, MP3 players, printers, home appliances, gadgets, etc. It would be useful if they could communicate with each other and provide added-value and meaningful services to their owners independent of their geographic location. This is the idea behind the concept of Personal Networks. A Personal Network (PN) [1], [2] is a person-centric, distributed environment of a person's devices, and provides access to personal resources and services regardless the location of the person. This is illustrated in Figure 19.1.

Figure 19.1: Example of a Personal Network.

Having a Personal Network with a variety of personal services and resources, one can benefit from sharing them with others in order to reach a common objective, for example sharing sensor information from different sources for rescue of people in disaster relief, getting real-time information from devices that belong to other persons in healthcare applications, sharing

digital media for business or entertainment. A Fednet is a secure group-oriented network composed of PNs, in which PNs collaborate with each other and share resources and services in a peer to peer (P2P) manner, i.e., they may be the producers and consumers of the services in the Fednet [3], [4], [5], [6].

Figure 19.2 illustrates the basic architecture of a Fednet. In this Fednet, the colleagues Alice and Kate staying in different locations federate their PNs to share camera view, videos and pictures related to their business affairs. Types of resources and services shared in Fednets vary depending on the application area. Each Fednet is tailored for a specific goal; therefore each Fednet has different characteristics.

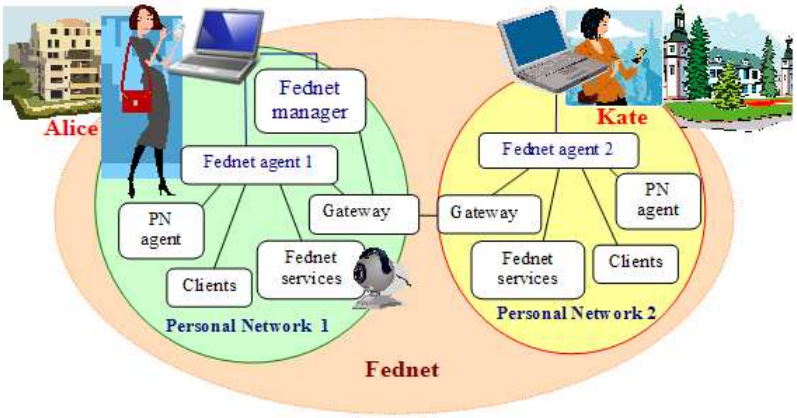


Figure 19.2: Basic architecture of a Fednet.

A Fednet is a dynamic entity, because it evolves incrementally as more PNs join, and it ceases to exist when all PNs leave it. Each PN has the Fednet agent functionality, which is responsible for joining/leaving a Fednet and controls access to personal resources and services of a PN. Furthermore, each Fednet has the Fednet manager functionality, which is responsible for management and control of the Fednet, such as creating, dissolving a Fednet and accepting/removing Fednet members. The Fednet manager functionality can be hosted by one of the PNs, as is illustrated in Figure 19.2, or can be provided externally by a third party.

When joining a Fednet, a PN obtains a membership credential signed by the Fednet manager. It contains the PN's name/pseudonym and its contact information. The membership credential has a validity period. Consequently, the credential should be periodically refreshed. This credential is used to au-

thenticate the PNs within this Fednet and for accessing the Fednet services. There are many possible situations in which the user can take advantage of using a PN and a Fednet. Figure 19.3 illustrates Alice's various activities that can be supported by the Fednets that her PN is engaged in.

Figure 19.3: Fednets support various activities of Alice.

a) Business (Office) Fednet: At work Alice attends a project meeting. In the office colleagues federate their PNs to prepare a project plan efficiently, by sharing important documents, photos, video clips, screen and presentation slides with each other. Furthermore, the PNs of Alice and her colleague Kate, from another affiliation of the company, are engaged in a Commercial Fednet. The commercial Fednet is established between the company's various affiliations from different cities to provide 'a virtual shopping mall' service to multiple customers and clients of the company from different cities.

b) Entertainment Fednet: Alice goes to a conference scheduled in another city by train. In the train, Alice federates her PN with another person's PN, who has the same hobby: collecting choreography of world dances. She shares the pictures and videos of her collection using her laptop with this

person, who shares with Alice fabulous photos and videos of Asian dance fragments.

c) Business (Conference) Fednet: Later at the conference, people with close research interests (e.g., marketing and selling products and goods) federate their PNs to make contact, to exchange documents, contacts and references, photos of the conference and other material, to conceive a business.

d) Educational Fednet. After the conference Alice wants to attend her distant learning course on modern art. Sitting in the hotel room, Alice federates her PN with her course-mates and attends the online course.

Here we can see how Alice's PN and various Fednets support her social life and daily activities. Note that while the essence of a PN is providing the user with personal ubiquitous services (e.g., Alice, can access her documents, course materials stored in her home PC from anywhere, in this case from the hotel), the essence of a Fednet is sharing these ubiquitous services with others for a common goal (e.g., Alice can share some of her documents with course-mates of her distance learning course to prepare an online assignment).

In this chapter, we address the issues of a dynamic access control to the services in a Fednet and stimulating the cooperation in Fednets. For this purpose we look at Fednets from a 'social' angle. Since behind each PN there is a person, i.e., the PN owner, the cooperation of the PNs reflects the social behavior of the PN owners, and therefore a Fednet can be seen as a social network of PNs. Reputation information is one of the driving forces in social networks. To enable a dynamic access control and a dynamic cooperation of PNs, we propose reputation-based framework for Fednets. We introduce the concept of a Federated reputation identity for Fednets/PNs, which enables them to collect and use reputation information across multiple Fednet domains.

The rest of this Chapter is organized as follows. In Section 2, we present the reputation-based framework for Fednets. In Section 3, we describe the operation of the reputation framework in Fednets. In Section 4, we discuss the results of the simulation which is being carried out to support the ongoing research. In Section 5, we briefly discuss the related work on reputation-based systems. Finally, in Section 6, we conclude and discuss future trends.

19.2 Reputation framework for Fednets

The core of the reputation-based system is the reputation information. Reputation built based on the experience of a single entity is called local reputation [7], also referred to as subjective reputation or first-hand information. Reputa-

tion built in cooperation, by all participants in the network, as a combination of all local reputations is called global reputation [7], also referred to as objective reputation.

19.2.1 Requirements to the system design

According to our observations in the literature [8] to benefit from using reputation, the design of a reputation-based system must meet minimum requirements, which we followed in our design.

1. The participants should collect feedback from their interaction experience and optionally can exchange or distribute their opinions to each other.
2. The source for observations must be identifiable, so that the reputation information can be accumulated for this source. The identities of the participants should be tracable, so that it should be possible to recognize them in the future interactions.
3. There should be a sufficient number of events/ interactions to acquire the experience and to learn the behavior.
4. Experience and observations must be factors in future decisions.
5. There should be incentives for the group members to collect and exchange their experiences during their interactions.

19.2.2 Reputation information in Fednets

If we see the reputation as an overall quality of interactions between the PNs, we can define the reputation as a previous interaction quality and the trust as a belief in future interaction quality. Building reputation information requires monitoring and observing the behavior of the participants. Reputation information is collected by all parties after every interaction. This local experience information is stored as credit points (or reputation value). These credit points are incremented when there is a positive experience and decremented when there is a negative experience. We define reputation for a PN, a PN's service and a Fednet in the context of Fednets.

Reputation of a PN is based on its service to other PNs, service consuming and cooperating behavior.

Reputation of a PN's service is based on the service's quality, content, availability, performance, price etc.

Reputation of a Fednet is the reputation that a PN concludes about the Fednet, based on the quality of cooperation experienced while being a member of this Fednet. It is a reputation that the Fednet has obtained from its members.

19.2.3 Building reputation in Fednets

In our framework, the PNs monitor each other and log their experiences. They report the local reputation value about other PNs to the reputation manager of the Fednet. As criteria for monitoring, evaluating the behavior and building a reputation for a PN in Fednets, we consider the interactions between the PNs and the contributions of the PNs to this Fednet. Interactions between the PNs are observed at the PNs. The primary information measured in any reputation-based system is the first-hand observation, i.e., the local reputation value. During the operation of the Fednet, the local reputation value is updated based on the number of successful interactions of the PNs and the satisfaction level of the PN owners. There are different ways to consider the interaction as successful, for example, system-level and user-level observations.

System-level observation is logging and counting of successful interactions by the Fednet. For example, the reputation of a service can be incremented, if the service response time is acceptable by the application. Furthermore, the local reputation of a PN can be increased, if the requested service was made available as it was promised.User-level observations are based on the quality of the service and satisfaction level of the user. This information is created by the user (PN owner)'s feedback on whether or not the quality of the service (provisioning) was satisfactory, after the service was delivered/consumed.

Observations on the contributions of the PNs are made at the Fednet manager which is aware of the amount and type of contribution of every PN in the Fednet. Initial reputation values can be assigned based on this contribution. If the contribution increases, the global reputation value increases as well.

19.2.4 Architecture of the reputation framework for Fednets

We motivate our choice for an architecture of the reputation-based framework based on the usability of the reputation information in long-term and short-term Fednets. For a reputation-based system, the duration of the cooperation of PNs is important, according to the Requirement 3 stated in Section 19.2.1. Let's consider long term and persistent cooperation of PNs in a Fednet. Long-

term and persistent cooperation of the Fednet members experiences several life-cycles before the Fednet's disbanding. Such cooperation allows to build the reputation information. Collecting and building up reputation information is more challenging in Fednets with a short-term cooperation between its members, especially, when the environment is dynamic, in which the PNs are anonymous and dynamically joining/leaving. In this case, we look beyond Fednets. If the reputation information is collected beyond a single Fednet at some commonly known entity, such as a reputation broker, then several Fednets can benefit from this reputation service. This will act as a federated reputation identity service provided by the reputation broker at a trusted third party (TTP). As a result, the PN can use its federated reputation account in other Fednets as well and can benefit from its collected reputation value in various short-term or long-term instances of Fednets. Based on these considerations, we propose a hierarchical reputation framework for Fednets. Figure 19.4 illustrates the location of the reputation framework components

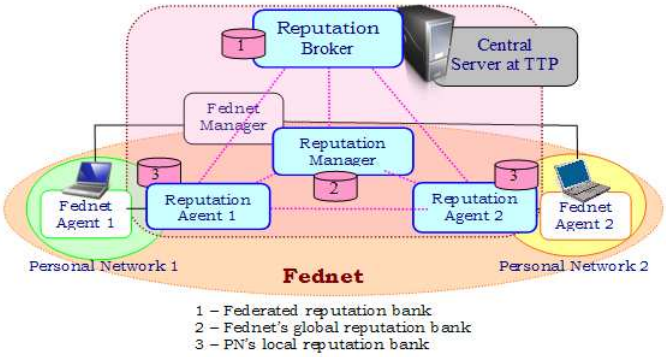


Figure 19.4: Reputation framework for a Fednet.

in the Fednet architecture. The reputation broker and its Federated Reputation Bank (1) are located at the TTP, an example of which can be the PN Directory Service proposed in [9]. The reputation manager can be located at the Fednet Manager (FM). The reputation manager maintains the Fednet's global reputation bank (2), which stores all information related to the reputation of the PNs and their services. At the bottom of the hierarchy are the reputation agents of the PNs. They can be located at the Fednet agent (FA) of the PN and maintain their own Local Reputation Banks (3). The local reputation bank of the PN contains the reputation information collected by the PN during the

participation of this PN in various Fednets. Participants of the system are the Fednets and the Fednet members and each of them have their reputation accounts in this system.

Reputation Agent is responsible for the following tasks:

- Monitoring, collecting the experience information from the participation of this PN in a Fednet. Moreover, it calculates the local reputation values for peer PNs, their services and the Fednets in which they took part and stores in its local reputation bank.
- Periodically, on demand or immediately after update, the reputation agent sends reports to the reputation manager of its Fednet on the reputation values collected about the peer PNs and their services based on the experience.
- Furthermore, when there is insufficient information, the reputation agent can request the reputation manager of its Fednet to provide additional information on the reputation of a particular service or a peer PN.

To implement the idea of reputation information, we define types of reputation as such: local reputation (LR) and global reputation (GR). Local reputation is based on the local observations of a single PN (Figure 19.5 a), and the global reputation is based on the observations of the group of PNs participating in the Fednet (Figure 19.5 b).

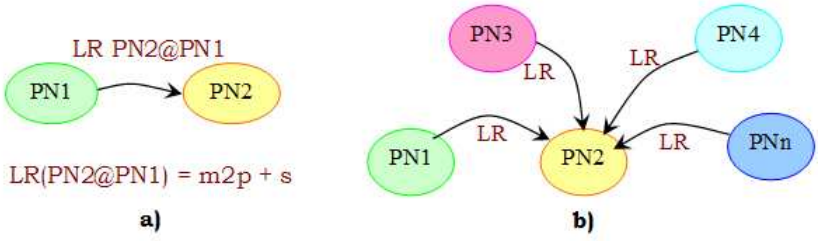


Figure 19.5: Local and global reputation of PN2.

LR2@1 is the reputation value of the PN2 calculated at the PN1 as is illustrated in Figure 19.5 a). It is the opinion of the PN1 about the PN2, built up from the experience with the PN2.

p is the number of the PN1's positive (successful) interactions with the PN2. If the number of successful interactions increases, the reputation value also increases.

m2 is a membership class of PN2 and it is indicated in the membership credential of PN2. Higher it is, higher will be the resulting reputation value, in addition, quicker the reputation grows.

S is a satisfaction level of the PN owners from the interaction: positive (1), neutral (0) and negative (-1).

The local reputation value for a Fednet at the RA:
LR (Fednet) = LRo + s (positive, neutral, negative)
Here LRo is previous or initial reputation value if available.

The local reputation value for a service at the RA:
LR (Service) = LRo + s (positive, neutral, negative)

Reputation Manager collects and stores the reputation information received from the Fednet participants about the PNs and their services. The reputation manager is responsible for:

- Calculating the global reputation in the Fednet domain based on the local reputation values provided by the reputation agents of the participating PNs.
- Maintaining the reputation information bank of the Fednet and storing the global reputation information.
- Making decisions on the access control to the Fednet by using the reputation value of the requesting PNs.
- Retrieving the reputation information from its bank, when there is a request from the reputation agent of some PN.
- Reporting to the reputation broker the collected reputation information during its operation. The reputation manager periodically uploads the reputation information of its participants to the reputation broker. Moreover, the global reputation information should be uploaded to the reputation broker when dissolving the Fednet.

The RM calculates the global reputation of the PN2 as follows:
GR (PN) = Contributions + Average SUM(LR) + Feedback index
Average summation of the reported LR values for the PN2:
Average SUM(LR for PN2) = 1/n (LR2@1 +LR2@3 + LR2@4 + + LR2@n)

Feedback index is a reward given to a PN by the RM for providing a feedback.

The RM calculates the global reputation of a service as an average summation of reported LR values for this service:
GR (Service) = Average SUM(LR)

The global reputation information is stored in the global reputation account, which contains the combination of the PN's pseudonym and its global reputation value, as for the service, it is a combination of the service's ID and its global reputation value.

Reputation Broker, an entity located outside the Fednet, is responsible for collecting the reputation information about the PNs and Fednets. It is a centralized functionality; therefore multiple Fednets and PNs can use the services of the same reputation broker. The reputation information at the reputation broker is federated reputation information accumulated for the PNs and the Fednets registered with this reputation broker. The reputation broker requires the PNs to register with their true identity. Here, we assume that the PNs and the Fednets register themselves with their true identity. This ensures that the identity of a PN can be traced by the reputation broker and this will allow building up the reputation scores for the PNs. However, the PNs can use different pseudonyms while joining different Fednets, so that they can preserve their anonymity within different Fednets. To prevent ambiguity, the reputation broker should control the uniqueness of the pseudonyms when registering PNs and Fednets. Although they can have multiple pseudonyms and their true identities are not revealed to others, they are still identifiable by the reputation broker. The reputation value the PNs obtain from their each cooperation and interaction in different Fednets will be accumulated at their single federated reputation account, since multiple (anonymous) pseudonyms of a PN are linked to the same federated reputation account. The federated reputation (FR) account contains the Fednet / PN name, pseudonyms and earned reputation values in different instances of Fednets. This account is dynamically updated based on the reports of the Fednets and the PNs.

The Fednet's FR value at the RB:
FR (Fednet) = Average SUM(LR) + Feedback index

The PN's FR value at the RB:
FR (PN) = Average SUM(GR) + Feedback index

Feedback index is a reward assigned to this Fednet / PN by the RB for providing a feedback. Reputation information at the reputation broker is collected not only during long-term cooperation but even in short-time cooperations of the PNs in various Fednets. Obtained credits in one Fednet can be utilized in other Fednets in the future. This is due Federated reputation identity (FRID) that contains the unique federated reputation account number and the federated reputation value.

FRID = (account number, reputation value)

19.3 Working of the reputation framework

We propose to use the reputation information in Fednets for service management and for rewarding of cooperative PNs.

19.3.1 Reputation-based service management

In our context, service management denotes admission control to the services, service discovery, selection and provisioning.

Reputation of PNs in the admission control

Reputation information can enable a dynamic admission control, which means that the access to the Fednet and its services is periodically adjusted based on the reputation values of the PNs. When joining the Fednet a PN presents its membership profile to the FM, which includes the PN's services list contributed to this Fednet. Once the PN joins the Fednet, the member list at the Fednet manager is updated with a new entry: PN name (ID), Contact info (IP of the FA), Service list, Membership class, Global reputation value. The membership credential of this PN, once created at joining the Fednet, is periodically refreshed and a PN will have new values for its global reputation in its subsequent membership credentials. Since the FM signs this membership credential, the reputation values can be verified by all members of the Fednet. The service offering PN can grant the access to its personal services based on the reputation of the service requesting/consuming PN stated in their membership credentials. Since the membership credential is adjusted from time-to-time based on the reported reputation values, eventually, cooperative PNs collect higher values of reputation; not cooperating PNs get less reputation; and misbehaving PNs get black-listed and isolated from the cooperation. As a result, the access rights also will be adjusted based on the reputation, i.e., higher the reputation values higher the access rights granted to the PN.

Reputation-based service discovery

The reputation-based service discovery is realized in the lookup service provided by the Fednet manager. The lookup response from the Fednet manager is a sorted list of services containing the information: Service name; Contact information; Popularity index of the service based on how often this service was requested; Reputation of the service based on the feedback of the other PNs.

In our design, a Fednet service requires certain reputation value (similar to the price) from its clients in order to allow access. Lower the reputation of the client-PN (e.g., number of contributions, number of positive feedback from peers), fewer services are visible to this PN in the lookup response list.

Reputation-based service selection

The services in the Fednets are rated based on their reputation value. When there are multiple instances of the same service in the Fednet, service consuming PNs can use the reputation of the service for choosing the best option. The reputation of the service is included in the lookup response list provided by the Fednet manager. When the user gets the list, it can sort it out based on the popularity and reputation. The user can also give preferences, so that the FA automatically sorts and chooses the service based on them. In addition, the reputation of the server-PN can also be used. The reputation of the server-PN can be retrieved during the authentication phase from the membership credential of the server-PN.

Reputation of PNs in service provisioning

Based on the reputation value of the PN, the policy evaluation produces a decision on service provisioning: either proxy-based or overlay-based service provisioning will be set up between the PNs. We consider two application environments: anonymous environment and a friendly environment for service provisioning in Fednets. In anonymous, privacy sensitive environment, the participants do not have sufficient reputation information about each other. In such an environment, we consider keeping the privacy of the users as a priority. In this case, we use reputation information for choosing the way of service provisioning in the Fednet. When there is a good established reputation in the community and the reputation values are high among the community members (above some threshold), then the focus of the service provisioning can be shifted towards better quality (less delay, less overhead, etc.). In this

case, the service provisioning can be done from any point in the PN that has the best link quality connection with the client PN.

19.3.2 Reward mechanisms to improve the quality of cooperation

The most effective way to stimulate the participants in group cooperation is reward [10]. Some examples of reward and incentive mechanisms reported in the literature are nuglets [11], virtual credits [12], traffic credits [13] and team based rewards [14]. To stimulate cooperation in Fednets we propose a reputation-based reward mechanisms for Fednets. Reward mechanisms in Fednets can be implemented in a distributed fashion, between the participants of the Fednet in a p2p manner without a trusted third party and in a centralized fashion, involving a third party (a reputation manager/broker).

Mutual reward - reputation tokens as a virtual currency
An example of a distributed reward mechanism is self-signed reputation tokens exchanged between the Fednet members. This approach is based on the reciprocity between the PNs, in which the reputation tokens play a role of non-monetary reward. The client PN1 gives a self-signed reputation token to the PN2 if the PN2's service was satisfactory. Eventually, while requesting a service from the PN1, the PN2 can present this token, signed by the PN1, to prove its reputation earned from the PN1. This mutual reward mechanism fits in ad hoc spontaneous 'Business Fednets' (Scenario c, Figure 19.3), created by special interest groups that share access to the resources and services such as internet access, printers, storage, processing, screens and various types of data. However, this approach does not scale to multiple Fednet domains, since the reputation tokens signed by one PN can not be presented to a PN from another Fednet.

Promotion - multiple domain service access
The usage of these collected reputation tokens can be extended to various PNs and multiple Fednet domains, when a trusted third party comes into the play. In this case, the reputation credits are collected by the third party and can be used as virtual payments even between anonymous PNs that participate in different Fednets. This allows earning (reputation-based) virtual currency in one Fednet and spending it in various other Fednets, supported by the same trusted third party or a chain of trusted parties. This is the idea behind the concept of the Federated reputation identity presented in Section 19.2.4. An example application for this case can be 'Commercial Fednet' in Figure 19.3,

created to enable virtual shopping malls in different cities, for selling personal items, community goods and company products. Suppose that Alice and Kate are the managers of the virtual shopping malls in different cities. The reputation managers of their Fednets keep the reputation scores for their members based on the quality of their services, and the satisfaction level of the customers. The reputation scores are reported by the reputation managers to the reputation broker, which creates Federated reputation identity for the participant PNs of these Fednets. The members, who earned high reputation values by advertising and providing the good quality services, will have their reputation class increased. As a reward, they will have the rights to access the services and to advertise their services in more areas and cities, i.e., will obtain broader range of discovery for their services in various virtual shopping malls.

19.4 Simulation

19.4.1 Scenario

We consider a scenario of communities, in which a large number of people want to sell their goods and also want to buy some products. The community members use their PNs to share their files and images of their products, which are various types of furniture, second hand sporting goods, home made handicrafts, unique pieces of art, etc. Each PN has a personal folder with a number of multimedia files describing particular products they are selling. They use file sharing to share multimedia files about the products for sale. The PNs based on their interest and experience can form Fednets, and can participate in multiple Fednets using different pseudonyms. Since anonymity is allowed, some people advertise bad quality goods. Therefore, the communities want to impose the admission control measures while forming Fednets and joining Fednets to increase the quality of goods that they offer to each other. In addition, the communities want to stimulate their members to behave in a cooperative way. We will address these issues with our reputation framework for Fednets. To test the reputation framework we will need a large number of participant PNs, having long or short term cooperation for building the reputation between them. We simulate various scenarios. The goal of the simulation is to prove the usability of the reputation framework in (a) admission control which can improve the quality of services; and (b) enforcing the cooperative behavior of the PN owners.

Behavioral strategies of PNs

Similar to the participants of the social networks, PNs in a Fednet might behave with different patterns to maximize the profit from the cooperation. We define three behavioral strategies of the PNs in a Fednet.

- Random behavior, may be caused by unreliable communication medium or by selection by the user.
- Cooperative behavior, always behaving honest and cooperating with others.
- Malicious behavior, we generalize here the behaviors such as non-cooperative, selfish, providing bad quality service intentionally, giving incorrect feedback about others.

To validate our design of the reputation-based framework, we focus on building reputations for the PNs with different behavior strategies, reputation in admission control and stimulating the member to cooperate.

Simulation parameters.

We implemented the simulator using Matlab with parameters:

- Behavioral strategies of PNs (random, cooperative, malicious);
- Membership class of the PN (unknown, familiar, trusted);
- Reputation class of the PN (bronze, silver, gold);
- Total number of interactions for each PN is 100;
- The number of positive interactions with other PNs is simulated;
- Satisfaction levels of the user are derived based on the interactions (positive, negative);
- Local, global and federated reputation values are calculated.

We suppose that there are 100 PNs, which are clients and servers in Fednets. There are three behavioral strategies for the PNs, random, cooperative and malicious. Cooperative PNs are 75, random behavior-PNs are 15 and malicious PNs are 10. PNs participate in different Fednets. Simulator each time chooses a random number of PNs to federate. Number of Fednets in the simulation setting is 100. Out of 100, 40 Fednets require silver and gold reputation class, which is in simulation settings as a minimum of 300 for the reputation value. Another 40 Fednets require minimum of 100 for the reputation value, which can be reached with bronze reputation class. The rest 20 Fednets can accept anyone. The PNs with low reputation might have chances to join these Fednets only.

Additional settings are:

- Adaptive malicious strategy, a PN that gets fewer opportunities to federate, hence access to fewer services, due to its behavior, changes its behavior to be cooperative. The reputation threshold value that forces the PNs to change the strategy to get admitted to the Fednets is taken as (-60)
- Fading of the reputation is 2%, which means if the PN does not contribute to the Fednet its reputation value will decrease for 2%. This is to make all PNs to participate in the Fednets and also to reduce the effect of reputation in the distant past.

After receiving a service the feedback is generated at the Reputation agent and a local reputation value is calculated. This local reputation value is reported to the Reputation manager and eventually to the Reputation broker, which also update the global and federated reputation values, respectedly. Local, global and federated reputation values are calculated using the formulas presented in Section 2.4. In these simulation settings, we assume that the reputation values are reported truthfully. The maximum reputation value for this simulation setting is 400 and minimum is -100. Admission to the Fednet is based on federated reputation information collected in previous Fednets. Higher the reputation means higher the chances to federate. We can see the reward here as the chance for admittance into the Fednets.

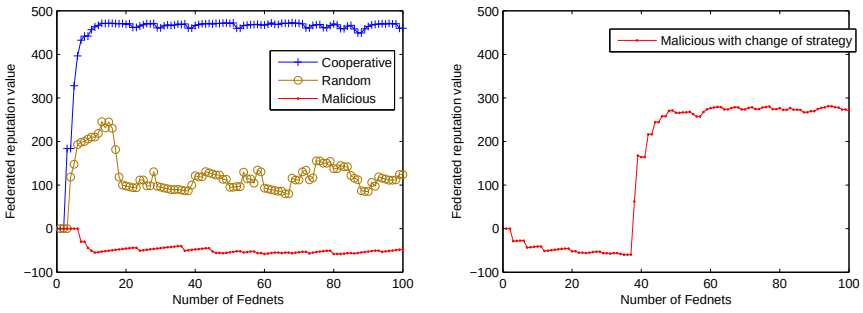
19.4.2 Simulation results and analysis

We analyze the results from the simulation run with respect to the following:

1. The reaction of the reputation system to different behavior strategies;
2. Admission into the future Fednets based on reputation that is built over a period;
3. Influence of the system to the change in the behavioral strategy.

Reputation for different behavioral strategies

Figure 19.6 illustrates the reaction of the reputation system to different behavioral strategies of the PNs. The reputation value is collected across multiple Fednets, so that it is accumulated as a federated reputation value for the PNs. Figure 19.6 a shows that the most profitable strategy to build the reputation is the cooperative strategy. Cooperative PNs build the highest federated reputation, while the malicious PNs will have their federated reputation reduced. When the PNs report truthfully, reputation information accurately estimates the real quality of the services delivered by the PNs in the Fed-



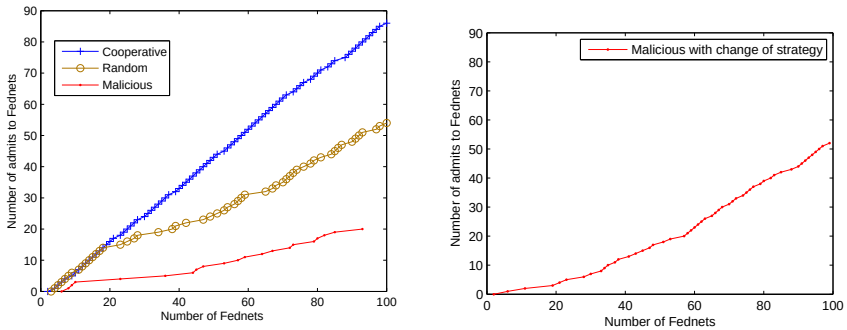
(a) (b)

Figure 19.6: Building federated reputation based on the strategy.

net. Furthermore, Figure 19.6 b demonstrates the influence of the reputation system to the behavioral patterns of the PNs. Malicious PNs, if it is adaptive, changes its strategy when its reputation reduces dismally. This is depicted in Figure 19.6 b with the increasing reputation value for the adaptive malicious PN. An important observation is that, even with changing the strategy, the adaptive malicious PNs never reach the same level as cooperative-only PNs. While cooperative PNs build up their reputation, malicious PNs decrease their reputation and the random strategy-PNs can expect unstable reputation within Fednets. Service failure or unsatisfactory service provisioning caused by the changing network conditions and circumstances is a typical situation for Fednet environment. Additional mechanisms will be required to distinguish the real cause of this random behavior, to prevent reduction of the reputation of an innocent PN.

Admission to the Fednet based on reputation

Federated reputation identity enables the mobility of reputation information across Fednets. When a member moves from one Fednet to another, or joins multiple Fednets, the PN's reputation earned in various Fednets is stored at the reputation broker, so that the PNs can accumulate and benefit from its reputation from multiple Fednets. Fednets admission control policy based on reputation information allows acceptance of a PN if the federated reputation of the PN is within the required range to join this Fednet. Figure 19.7 illustrates the admission to the Fednet based on the reputation built due to the behavioral strategies of the PNs. The PNs with high reputation values (coop-



(a) (b)

Figure 19.7: Admission control based on the behavioral strategies of PNs.

erative PNs) have a chance to join the maximum available Fednets. While the PNs with the lower reputation values (non-cooperative PNs) will end up with less possibilities.

Stimulating the good behavioral strategy

We consider that the reputation-based admission to a Fednet is a reward for the PNs for their good reputation. This reward gives incentives for the PNs to cooperate and increase their reputation. When a non-cooperative PN is continuously having fewer opportunities to join other Fednets, the PN will be urged to behave rationally, so that it will try to increase its reputation. This is also stimulation for the PNs for better cooperation. Figure 19.6 b illustrates that reputation below a certain threshold forces the PN to change its strategy from malicious to cooperative. After changing the strategy, the PN increases its chances to federate with others, as is illustrated in Figure 19.7 b.

19.4.3 Discussion

Due to the centralized collection of the reputation, the short-term Fednets can also benefit from using reputation. This is demonstrated in Figure 19.6, which proves the usefulness of the framework in the run of 100 short-term Fednets. Figure 19.7 demonstrates that reputations can be efficiently used for admission control in Fednets. The added value of the reputation-based framework here is dynamic and flexible access control and incentives for the PNs to obtain higher reputations that affect the quality of their cooperation.

The system copes with the malicious behavior by reducing chances to federate with others or to join Fednets. This can help the Fednets to reduce the selfish behavior of the PN owners. These are our initial results in designing and simulating reputation-based framework for Fednets. The work is on to track the inconsistent behavior, i.e., manipulative behavior in different Fednets to get maximum profit from the cooperation. The issues related to overhead and complexity of the reputation framework taking into account the issues from untrustful feedback of the PNs need to be looked into.

19.5 Related work

A lot of interesting works have been reported in the literature on reputation-based systems. These systems tackle different problems in different layers, starting from the networking and routing to the services and applications [8]. In this Section, we discuss some of the reputation-based systems and compare their approaches with ours. The reference [15] proposes a dynamic incentive mechanism to motivate the personal network nodes in participating in cooperative relaying. As a reward for cooperative behavior, the nodes receive additional throughput based on reputation calculations for individual contributions. Dynamic assignment of the reward prevents the nodes from adversely manipulating their behavior after getting the reward.

In [12] the reputation information is used in improving the quality of service provided by the ISPs in wireless hotspot environments. After the receiving a service from ISP, the mobile node sends to the Trusted Certification Authority (TCA) its feedback on the service received from ISP. Based on the feedback the TCA issues a new certificate with the updated reputation value of the ISP. While the incentives for the ISPs to get more clients, the incentives for the mobile nodes are to receive a better service and some amount of credit from their home ISP for feedback.

Another interesting approach discussed in [16] is based on penalty. An independent reputation mechanism requests binary feedback about interactions, 1 for high quality service and 0 for low quality service. The reputation of a provider is computed as an average satisfaction rate of the clients for a given period of time. At the end of each period, the reputation mechanism publishes the reputation of every provider, and service providers are expected to refund every client the monetary penalty specified in the SLA. When penalty is large enough, [16] proves that rational service providers keep their promises.

While [15] focuses on the single service, i.e., the forwarding service between the PNs, our goal is to assist the PNs and Fednets in selecting the

reliable PNs and Fednets to federate, based on the satisfaction level from previous interactions. In [15] reputation mechanisms should be implemented in each node participating in cooperative relay process, i.e., user terminals, relays and base stations. In [12] and [16] reputation mechanisms should be implemented in user terminals and in the infrastructure. Our approach has less complexity, since the reputation mechanisms can be co-located with the existing Fednet functionalities, the Fednet Agent and the Fednet Manager. The only additional functionality that is required for the centralized reputation collection is the reputation broker functionality at a trusted third party. All systems [15], [12] and [16] use centralized mechanisms for reward and punishment, while our approach is hierarchical: distributed in a Fednet domain and centralized across multiple Fednet domains. This makes our system scalable, since the system can be used within single Fednets independently and between multiple Fednets cooperatively.

19.6 Conclusion and future trends

In Fednets, motivating the members to cooperate is a challenge. We address this challenge with a reputation-based approach. A reputation-based system motivates the participants to obtain a good reputation in order to benefit from the cooperation. Using the reputation can help to bring the system into balance. For example, by using reputation in the system, the good members get rewarded for their good behavior and the bad members get punished. As a consequence, the members are motivated to behave well, e.g., to cooperate and share their resources. With time, the effect of this reward and punishment will be seen as self-healing, i.e., getting rid of malicious, non-cooperative behavior, since this behavior will become irrational.

In this chapter, we presented a reputation-based framework for Fednets and showed how the Fednets can benefit from using reputations in service management and improving the quality of cooperation between the PNs. The framework provides a dynamic access control in Fednets, which means that the access control to the Fednet membership and resources, is periodically adjusted based on the reputation values of the PNs, i.e., higher the reputation value higher the access rights of these PNs.

Although the requirements to the reputation-based systems state, that the Fednets should have a long-term and stateful cooperation of the PNs, we argue, that even short-term and stateless cooperation of PNs in a Fednet can benefit from using reputation and social control. We introduced a reputation broker functionality that operates beyond the Fednets and serves multiple

Fednets and PNs as a trusted reputation authority. We introduced the federated reputation identity for the PNs and the Fednets, which is a service provided by the reputation broker located at the TTP. The reputation broker functionality makes the system scalable and applicable for multiple Fednets linked with a common third party (or a chain of trusted third parties). The simulation results proved the usability of the reputation framework for admission control and for stimulating cooperation in Fednets. The results presented in this chapter reflect our initial research on applying reputation in Fednets, which is a promising and interesting avenue for further research.

In the future, managing large number of personal devices will be a challenge and an important issue for the users. The users are becoming providers and consumers of the services. In this sense, Fednets will become attractive to the users, since they are of Personal Networks, can be operated independently from the operators, can be suitable in various scenarios, can support various types of group-oriented applications tailored for infotainment, communication and collaboration, distributed computation, internet service support and content distribution, remote healthcare and social networking and finally, can support the social life and business activities of PN owners.

The advantages of Personal Networks and their federations will become more obvious as the number of personal devices increases. Although nowadays we have just a few devices, in the near future this number is expected to increase tremendously. It is predicted by the Wireless World Research Forum [17] that, 10 years from now, there will be 7 trillion wireless devices serving 7 billion people, that is, an average of 1000 wireless devices per person. The proliferation of all types of sensors and portable devices with networking facilities will result in new paradigms for service delivery models and service architectures. Fednets are an example of them. Personal networks and their federations can be seen as a next generation networking concept with service-orientation and personalization features: the concept that allows users to share their personal services in a seamless, secure and flexible way; the concept that allows organizing a big part of personal devices in order to make them cooperate in an effective way and provide next generation services.

References

[1] I. G. Niemegeers and S. M. Heemstra de Groot, “Research issues in ad-hoc distributed personal networking,” *Wireless Personal Communications*, vol. 26, no. 2, pp. 149–167, 2003.

[2] PNP2008, "The dutch freeband communications project personal network pilot 2008," www.freeband.nl, 2004-2008.

[3] I. Niemegeers and S. Heemstra De Groot, "Fednets: Context-aware ad-hoc network federations," *Wireless Personal Communications*, vol. 33, no. 3, pp. 305–318, 2005.

[4] M. Ibrohimovna and S. Heemstra De Groot, "Proxy-Based Fednets for Sharing Personal Services in Distributed Environments," in *Proc. Fourth Int. Conf. Wireless and Mobile Communications ICWMC '08*, 2008, pp. 150–157.

[5] Ibrohimovna, M. and Heemstra De Groot, S.M., "Policy-Based Hybrid Approach to Service Provisioning in Federations of Personal Networks," in *Proc. Third Int. Conf. Mobile Ubiquitous Computing, Systems, Services and Technologies UBICOMM '09*, 2009, pp. 311–317.

[6] M. Ibrohimovna and S. Heemstra De Groot, *Handbook of Research on P2P and Grid Systems for Service-Oriented Computing: Models, Methodologies and Applications*. IGI Global, January 2010, ch. Fednets: P2P Cooperation of Personal Networks, Access control and management framework, released: January 2010. ISBN: 161520686-8.

[7] H. Massum and Y. Zhang, "Manifesto for the reputation society," *peer reviewed journal of the Internet First Monday*, vol. 9, 2004.

[8] M. Ibrohimovna and S. H. de Groot, "Reputation-based systems within computer networks," *Internet and Web Applications and Services, International Conference on*, vol. 0, pp. 96–101, 2010.

[9] MAGNET, "Ist 6fp project my adaptive global network," www.ist-magnet.org, 2006-2008.

[10] D. G. Rand, A. Dreber, T. Ellingsen, D. Fudenberg, and M. A. Nowak, "Positive interactions promote public cooperation," *Science*, vol. 325, pp. 1272–1275, 2009.

[11] L. Buttyan and H. J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *ACM/Kluwer Mobile Networks and Applications (MONET*, vol. 8, pp. 579–592, 2003.

[12] N. B. Salem, J.-P. Hubaux, and M. Jakobsson, "Reputation-based wi-fi deployment," *Mobile Computing and Communications Review*, vol. 9, pp. 69–81, 2005.

[13] A. Weyland, T. Staub, and T. Braun, "Comparison of incentive-based cooperation strategies for hybrid networks," in *WWIC*, 2005, pp. 169–180.

[14] E. C. Efstathiou, P. A. Frangoudis, and G. C. Polyzos, "Stimulating Participation in Wireless Community Networks," in *Proc. 25th IEEE Int. Conf. Computer Communications INFOCOM 2006*, 2006, pp. 1–13.

[15] J. Hwang, A. Shin, and H. Yoon, "Dynamic reputation-based incentive mechanism considering heterogeneous networks," in *PM2HW2N '08: Proceedings of the 3nd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*. New York, NY, USA: ACM, 2008, pp. 137–144.

[16] R. Jurca and B. Faltings, "Reputation-based service level agreements for web services," in *In Proc. of the 3rd International Conference on Service Oriented Computing*, 2005, pp. 396–409.

[17] N. Jefferies, "Global vision for a wireless world," Wireless World Research Forum, 18th WWRF meeting, June 2007, helsinki, Finland.