2010 Fifth International Conference on Internet and Web Applications and Services

Reputation-based Systems within Computer Networks

Malohat Ibrohimovna
Delft University of Technology,
The Netherlands

m.kamilova@tudelft.nl

Sonia Heemstra de Groot
Delft University of Technology,
Twente Institute of Wireless and Mobile
Communications, The Netherlands
sonia.heemstra.de.groot@ti-wmc.nl

***Abstract*—the topic on using reputation has received considerable research attention in the field of networking and communications. In this survey paper, we discuss the various ways the systems can benefit from using reputation information. We provide the examples of existing reputation-based systems discussing their functional implementations. Based on our observations, we list minimum requirements for benefiting from reputation-based systems in computer networks. This survey is suited as a tutorial for both researchers and practitioners, willing to build reputation systems, equipped with the knowledge and experience have been made in the field.**

Keywords- reputation, reputation-based systems.

I. INTRODUCTION

Computer networks were built to support human networks imitating their characteristics. One of the characteristics of human networks is that the relationships are adjusted based on the interaction experience, trust and reputation between the group members. In reputation-based system, the experiences create opinions about others, which are then 'transformed' into reputations. Having reputation information one can judge the situation, estimate the future outcome from the cooperation and decide whether to cooperate or not. Similar to human networks, in computer networks, the group members can benefit from exchanging the reputation information they have collected, because the experience of others can facilitate the decision process. Furthermore, a reputation-based system motivates the group members to obtain a good reputation in order to benefit from the cooperation. In order to get a reward, the members are motivated to be honest, trustful and to provide a good service to each other.

A brief introduction to reputation information in computer networks. The core of the reputation-based system is the *reputation information*. Reputation is a belief derived from previous interactions with an entity that the entity will behave in a certain expected way. It is the subjective knowledge about the entity's past behavior which gives certain expectations about its future behavior. Reputation can be built based on the experience of a single entity, and this type of reputation information is called *a local reputation* [1]. In some sources it is called *a subjective reputation* or first-hand information. Reputation which is built in cooperation, by all participants in the network, as a combination of all local reputations, is called *a global reputation* [1]. In some sources it is called *an objective reputation.* Both of them have advantages and disadvantages. For example, the advantages of local reputation are the following: It is *trustful*, because it is based on its own experience of an entity; It is *consistent*, because it is based on the same set of criteria. However, the disadvantages are: it takes a *long time* to be built and to benefit from using it; It has a *limited scope*, as it is based on the experience and perception of a single entity; and therefore it is *subjective* in comparison with the global reputation.

The advantages of global reputation are: it gives an *objective* and global view to the situation, to the behavior of the entities; It *saves time* and efforts in processing and analysis of collected information. However, the disadvantages are: "*Majority wins*" means that there can be wrong accusations, incorrect ratings, attacks such as brainwashing, intoxication [2]. Moreover, to compute the global reputation value, the local reputation information needs to be exchanged between the participants, and therefore it creates *overhead*, *inconsistency* and *scalability* problems.

How the systems can benefit from using reputation information? In this paper, we provide a survey on reputation-based systems from various fields of computer networking. Furthermore, we investigate the ways the reputation information is used to stimulate the cooperative group behavior and to improve the quality of cooperation in these systems. This paper is organized as follows. In Section II, we discuss examples of the existing reputation-based systems. In section III, we present our observations from the survey and summarize the survey in Section IV.

II. REPUTATION IN VARIOUS SCENARIOS

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 [3-21]. In this Section, we discuss how the reputation information helps in decision making process; how it is used to implement a reward system and how it improves the quality of cooperation in these systems. We start our survey with the watchdog system, the first simple system have been

978-0-7695-4022-1/10 $26.00 © 2010 IEEE
DOI 10.1109/ICIW.2010.22

proposed to tackle the problem of selfish nodes in computer networks.

A. *Encouraging routing and forwarding behavior*

In *Watchdog and Pathrater* [3] shown in Figure 1, the problem of selfish nodes is addressed. Each node in the network has its own watchdog component for monitoring the neighbors and a Pathrater component to choose for the route which excludes non-forwarding selfish nodes. The results of the observations by each node are not distributed to the neighbors. The performance of the network is improved in forwarding, by excluding the selfish nodes. However, The drawback of this system is that there is no reward and no punishment for the participants. Consequently, the selfish nodes still can forward their packets via others, while they are relieved of forwarding the packets of others. So that it becomes even advantageous to be selfish. This drawback is addressed in the subsequent systems.

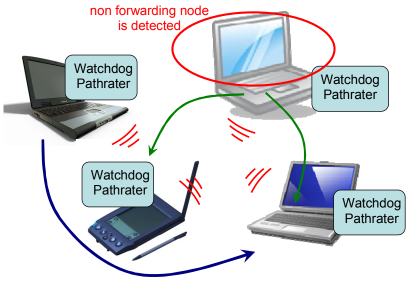


Figure 1. Watchdog and Pathrater

CONFIDANT (COoperation of Nodes: Fairness In Dynamic Ad-hoc NeTworks) [6] is a collaborative watchdog mechanism using reputation information. The nodes keep the records on the reputation and trust and exchange their observations with each other. The nodes that are detected to be selfish are not used for forwarding and routing. In addition, their packets are also not forwarded and routed by other nodes, as is illustrated in Figure 2.

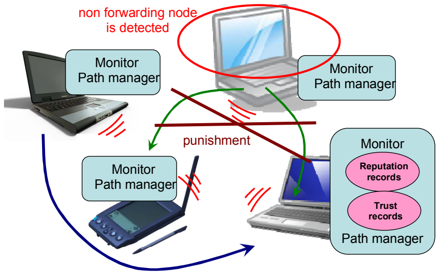


Figure 2. CONFIDANT

Consequently, they become isolated from the network, as a punishment for being selfish. This forces the nodes to forward the packets of others and to serve others, if they want to be served themselves.

CORE (Collaborative Reputation) [4] is another system that complements the watchdog mechanism with reputation information, so that the neighbor's opinions are taken into account. Differently from the previous system, in CORE only the positive reputation information is exchanged and only by request. A combined reputation value is derived from: a) subjective reputation, built from local observations; b) indirect reputation, built from positive records of others; c) functional reputation, derived from the task specific behavior of the node. Higher the collaborative reputation of the node better its network connectivity.

SORI (Secure and Objective Reputation-Based Incentive) [5] tackles the problem of selfish nodes with non-forwarding misbehavior and uses a monitoring mechanism similar to the watchdog. The reputation of a node is quantified taking into account the neighbors monitoring. Reputation ratings are forwarded locally, propagated only to the neighbors. Received reputation ratings are authenticated by a one-way hash-chain. The incentive for a selfish node is to keep a desirable quality of its network connectivity. This way the system encourages the forwarding behavior of the nodes.

PARS (Power-Aware Reputation System) [7] is the system, compatible with any reputation system. It is designed to be used on top of existing models which try to solve non-forwarding issues, such as CONFIDANT and CORE. PARS tries to solve the problem of false energy announcements, i.e. misreporting lower energy by a node in order to save energy. Two types of reputation are distinguished in the system: *energy related reputation and data-forwarding reputation*. The reputation of the node is higher when it has higher energy. The system is distributed. Each node has Detection module to detect energy misreporting behavior of the node and Jury module to 'judge' and collectively isolate a 'convicted' node. The goal of the system is to stimulate cooperation of nodes in routing in ad-hoc networks. By assigning punishment for false reports, the system provides incentives for the nodes to be honest in their cooperation.

In the above discussed systems there is no explicit reward for a good behavior. The reward implicitly can be considered as "having better connectivity". The reference [8] 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. The motivation for a dynamic assignment of the reward is to prevent the nodes from adversely manipulating their behavior after getting the reward. To achieve a dynamic incentive mechanism, the authors propose to add a bonus (incentive) parameter in the allocation of the timeslot by the time-division high-data-rate system scheduler. The bonus parameter contains two variables. The first is the initial fixed throughput reward, which depends on the service provider's business model.

The second is the dynamic value, based on the assistance of the node in the cooperative relay service. Each end user calculates and periodically reports to the base station the reputation of each relay node that has contributed to traffic transmission. The Base station derives the reputation value for each relay node and based on it rewards additional throughput to each cooperative relay.

B. Reputation in sharing sensor information

In [9] the goal of using the reputation in the system is to exclude from the network malicious beacon nodes. Reputation information helps to distinguish between trusted and malicious beacon nodes which provide false location information. The reputation information is local and is stored in each beacon node and each sensor node, hence the system is distributed. Each beacon node maintains a neighbor reputation table, which is updated based on the monitoring of one-hop neighbor beacon nodes for misbehaving. The sensor node uses the data from these neighbor reputation-tables, and based on a simple majority voting scheme, determines trusted beacons and stores this information in trusted beacon neighbor tables. Consequently, using reputation information sensor nodes can choose to whom to believe for the location information.

In [10] the goal of using the reputation is to evaluate the trustworthiness of the nodes by observing their behavior in data forwarding and the consistency of the sensed data. Every sensor node has a watchdog mechanism which monitors the others and locally maintains the reputation information about other nodes. The reputation information is derived from the local observations and second hand information, i.e. the observations of other sensor nodes. Based on the reputation the sensor nodes decide whether to collaborate with particular sensor node or not. However, there is no explicit reward in these systems.

C. Reputation in improving the quality of service in wireless hotspots

Nowadays, different ISPs in a wireless hotspot compete to attract more clients. How to motivate them to provide a better service to mobile nodes and how to help the mobile nodes to choose for the best ISP in the wireless hotspot? In [11] the reputation information is used in improving the quality of service provided by the ISPs in wireless hotspot environments. This is a centralized model of a reputation-based system, with economic incentives for the participants. Figure 3 illustrates how the system works.

The reputation records are stored in the Trusted Certification Authority (TCA), which generates keys for ISPs, Mobile nodes and Home ISPs. TCA is a central entity with whom the ISP's register themselves. TCA issues each ISP with a certificate where the reputation value for the ISP is signed with the private key of the TCA. The ISP presents this certificate to its clients when it offers its services.

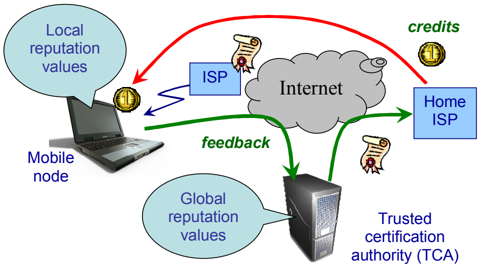


Figure 3. Reputation-based system for wireless hotspots

The mobile nodes can verify the certificate with the public key of the TCA. After the receiving a service from ISP, the mobile node sends to the 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 and sends it to the ISP. Then the TCA informs the Home ISP that the mobile node gave its feedback. The Home ISP rewards the mobile node with some amount of credit. The incentives for ISPs are to get more clients by having a good reputation, while for the mobile nodes the incentives are to get a better service and some credits from their Home ISPs. Here there is mutual reward, so both the clients and the ISPs have incentives.

Another interesting approach is discussed in [20]. An independent reputation mechanism requests binary feedback about interactions, 1 for a 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. When clients report truthfully, reputation information accurately estimates the real quality of the services delivered by the provider in that period. 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. The penalty is positive if the delivered quality of service is lower than advertised and zero otherwise. Here we can see that the reputation of the provider is derived from the quality of service it has provided in a particular period. When penalty is large enough, [21] proves that rational service providers keep their promises and the market is efficient.

D. Reputation in sharing wireless access

The reference [12] proposes a P2P Wireless Networks Confederation (P2PWNC) protocol, which encourages cooperation in Wireless community networks (WCN). It is based on the reciprocity (mutuality) algorithm that stimulates participation in WCN. The meaning of the reciprocity is that the system requires contribution before consumption, so that the consumption and the contribution should be balanced. The entities used in the protocol are: digital receipts, receipt servers and teams. *Digital receipts* are the evidence that WLAN service was contributed or consumed. Users sign digital receipts when they use the services. *Receipt servers* store the receipts generated by users after each WLAN session. The protocol supports both distributed (one server for all teams) and centralized servers (one per each team).

The system uses *teams* instead of individuals in order to make the architecture oriented to teams, so that the reciprocity is based on the team and not on the individual. In this group-oriented architecture some of the team members may reside in the areas with few numbers of mobile nodes, whereas others may reside in densely occupied areas. Team-orientation allows abstracting the individuals into a team. However, this makes a room for free-riders in a team.

The system allows the nodes to have multiple and free IDs with no registration, which provides total anonymity. However, anonymous IDs make the recognition of the peers difficult or not possible at all, which also leads to the problem of free-riders.

E. Reputation in P2P file sharing networks

Reputation is used in P2P systems to determine the peers which offer best quality resources and services, and to rate the quality of the offered resources. Moreover, the reputation information is used also to determine the peers which provide the most reliable information about other peers and their resources, which is called the *credibility* of a peer.

The work [14] describes self-regulating system, where the P2P network is used to implement a reputation mechanism. The system is distributed and allows assigning, sharing, as well as combining reputations on servents and resources in Gnutella-like environments. Servent is a node, which is a client and a server at the same time. Each peer maintains two experience repositories to store local reputation values. One is a resource repository, to store the resource's reputation, whether the resource is good or bad in the peer's opinion. Another is a servent repository, to store a servent's reputation, i.e. the number of successful or unsuccessful downloads from the servent. The opinions of peers are weighted by their credibility, which is separate from their trust ratings to avoid the malicious peers to be supported by the peers with strong reputation. The whole process is carried out in this way: resource searching and selection, vote polling and evaluation, best servent selection and resource downloading.

The reference [15] describes the trust management used to prevent the spread of malicious content in P2P networks. A reputation-based trust management protocol selects the files to download from peers who have higher ratings of reputation. The system uses trust vectors, calculated from the subjective opinion of peers, derived from their past interactions with peers. Opinions of peers are also weighted by their credibility. Each time a peer completes the downloading a file, the user is requested to judge the file for being good or malicious. When the file is judged as good, the rating of the peer from which the file is downloaded is upgraded. In addition, the trust and credibility values for the peer who recommended this file are also upgraded.

The work [16] proposes a reputation-based framework with a trust model quantifying and comparing the trustworthiness of peers based on the transaction-based feedback system. Trust evaluation is performed in a dynamic and decentralized manner at each peer, by the trust manager, which collects trust data about the peer and computes the trust value. The evaluation of the trustworthiness of a peer is based on the factors, such as peer feedback (satisfactory or not), number of transactions, credibility of the feedback source, transaction context factor (context dependent information) and community context factor (reward for submitting feedback).

KARMA [17] is an economic framework to be used in file sharing applications in P2P networks as a complementary system for discouraging free-riding behavior. The aim of the framework is to help P2P systems to achieve parity between the resources contribution and consumption of the peers. "Karma" is a scalar value, which is the peer's overall standing in the global system. Peers possess some amount of karma in their accounts, which is increased or decreased if the resource is contributed or consumed, accordingly. Peers should keep track of the account balance, since if there is insufficient karma the peer will not get a service. The major disadvantage of the system is that the peer can repeatedly join the system and each time can obtain a start up amount of karma. The system can only limit the rate of repeatedly joining behavior.

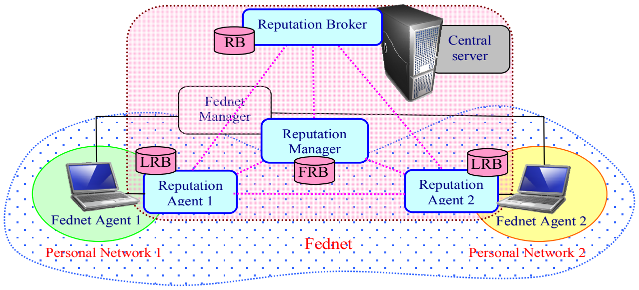
The work [13] presents a stamp trading system, in which 'stamps' are used instead of reputations. The value of the stamp represents the ability of a peer to use the network. Receiving a stamp can be seen as a payment equal to the stamps value. The stamps can be redeemed in the transactions between the peers. The peers need a sufficient amount of stamps to be able to get a service they require, however, the value of the stamp also depends on the stamp exchange rates. With negative experience with the peer, the peer's stamp exchange rate will fall. If its stamps fall in their value, then others will not want to purchase these stamps. According to [13] the stamp trading has a flavor of both reputation and payment, so that the *stamp trading protocol* is a generalization of both. When the node trusts that a stamp will be redeemed, it bases its trust on the *reputation* value, and when the node receives the stamp, this can be seen as a *payment* equal to the stamp's value. However, the difference is that the reputation can be earned and lost, rather than bought and sold.

F. Reputation in vehicular networks

The reference [18] proposes a reputation-based system for exchanging the information to increase traffic safety and improve mobility in vehicular ad-hoc networks. The main idea is 'opinion piggybacking', i.e. while distributing and forwarding an event message, every forwarding node appends to the message its own generated opinion about the message's trustworthiness. The opinion is derived a) from the experience of detecting this event, b) from the opinions of others, called partial opinions and c) from the trust value of the sender if it is known. The opinion exchange enables the confident decision on event messages. This reputation-based system is designed to be used in large adhoc networks consisting of highly mobile nodes.

G. Reputation in Fednets

Fednet, a federation of personal networks (PNs) [19] is a p2p cooperation of PNs. Figure 4 illustrates the reputation framework for Fednets.



RB – Reputation bank; FRB – Fednet's reputation bank; LRB – PN's local reputation bank

Figure 4. Reputation framework for a Fednet

The reputation broker is a centralized functionality which can be located at a Trusted Third Party. Reputation broker maintains Federated Reputation ID for PNs and Fednets, to enable them to collect the reputation information not only during long-term cooperation but even across short-time cooperations of PNs in multiple Fednets. The reputation manager maintains all information related to the reputation of the PNs and their services, while the reputation agents maintain the reputation information collected by the PNs during the participation in various Fednets. Participants of the system are the PNs and each of them have their reputation accounts. The PNs collect reputation information and the system uses it for its decisions in access control, service selection, load balancing and rewarding cooperation of the PNs. Due to the reputation framework, 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 this PNs.

III. OBSERVATIONS

In our survey, we observed that the goal and the range of the usage of the reputation information is broad. Some systems use reputation information to detect:

- *selfish nodes* with non-forwarding misbehavior;
- *malicious nodes* distributing malicious content during file sharing ;
- *cheating nodes* spreading non trustful information about others;
- *non-fair* nodes, who try to consume more and offer less.

The goal is to improve the quality of cooperation between the participants of the system.

In other cases, the reputation information helps the entity to choose the best available option based on the reputation value. The goal here is to stimulate cooperation and to motivate good behavior, since good behavior becomes beneficial.

Our observations showed us that there are minimum requirements that should be met to benefit from reputation-based system. We summarize them as follows:

A. There should be *sufficient number of events*/ interactions to acquire the experience and to learn the behavior. Otherwise, the reputation information can not be collected due to the short and temporal existence of the cooperation;

B. The participants should observe each other's behavior and *collect the feedback* from the interaction experience [22]. Optionally, depending on the application and the purpose, the participants can *exchange or distribute* their opinions to each other. However, this requires a reputation calculation engine and reputation exchange protocol in the system.

C. The *source* for observations must be *identifiable*, so that the reputation information can be accumulated for this source. Or the identities of the participants should be kept unchanged, so that it should be possible to recognize them in the future interactions. They might join and leave the group, but regularly come back to join the group or to use its service - so that previously collected information about them can be used to control the access to the group and its services. The participants must be identifiable when they join back to the group or request the service. This is described in [22] as: "long-lived entities that inspire and expectation of future interactions".

D. *Experience and observations* must have effect in future decisions, so that the accumulated knowledge should be used to facilitate future decisions. The participants collect reputations, exchange and use them for making decisions (e.g., on the access control).

E. The participants should have *incentives* to monitor each other and exchange their observations with each other.

IV. SUMMARY

In this paper, we provided a survey on some of the existing reputation-based systems in computer networks. The purpose of this survey is to study the application of reputation information in various scenarios and the benefits the systems gain from using the reputation information.

We started our journey with first and simplest mechanism, Watchdog and Pathrater, which was designed for detecting non forwarding behavior and avoiding this node in packet forwarding, where simple local ratings are collected at each node. The lack of reward and punishment in the system which encourages free-riding necessitated the further development of the simple watchdog scheme, by adding additional mechanisms, such as reputation and trust, reward and punishment, fading of the reputation information, and using more complex representation for the reputation, such as *subjective* reputation, *indirect* reputation, *functional* reputation, *energy-related* reputation and *data-forwarding* reputation. Later systems introduced the term of *credibility, trust* and *trustworthiness*.

The reputation information in a group communication can bring positive effects, such as:

- incentives to cooperate and behave good;
- fairness in the system by using reward and punishment for certain behavior, e.g., preventing free riding;
- improving the network connectivity, the quality of services and content in the system, by means of excluding the malicious peers and their content from the network;
- denying service or cooperation and isolating the malicious nodes and peers, so that they can not use the network services until their reputation becomes tolerable.

Consequently, the use of the reputation information in the system improves the quality of cooperation between the group members.

However, the reputation information can also bring negative effects to the system, such as the risk of rumors, brainwashing [2], being falsely accused or being undetected and other attacks, which affects the performance, reliability and usability of the reputation-based approach. Therefore, a reputation-based system should be designed carefully, keeping in mind the requirements listed in Section V and taking into account its drawbacks as well as its benefits.

REFERENCES

[1] H. Massum and Y.Zhang, “Manifesto for the Reputation Society”, peer reviewed journal o the internet, First Monday, 9/7, July 2004. http://131.193.153.231/www/issues/issue9_7/masum/index.html (last visited 26.06.2009)

[2] S. Buchegger and J.Y. Le Boudec “Self-policing Mobile ad hoc networks by reputation systems”, IEEE Com.Magazine, 43(7):101--107, July 2005.

[3] S.Marti, T.Giuli, K.Lai, M.Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, Proc. MOBICOM 2000, pp.255-265.

[4] P. Michiardi and R. Molva, “Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” In Proc. IFIP TC6/TC11 Conference on Communications and Multimedia Security, Slovenia, 2002, pp.107-121.

[5] Q. He, D.Wu and P. Khosla, “SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad hoc Networks,” in Proc. of IEEE Wireless Communications and Networking Conference (WCNC2004), Atlanta, GA, USA, March 2004, pp. 825–830.

[6] S. Buchegger and J.Y. Le Boudec, “Performance analysis of the Confidant protocol cooperation of nodes–fairness in dynamic ad-hoc networks,” In Proc. of MobiHoc 2002, Switzerland.pp.226-236.

[7] Dong Lu, Haitao Wu, Qian Zhang, Wenwu Zhu, PARS: Stimulating Cooperation for Power-Aware Routing in Ad-Hoc Networks, IEEE ICC’05, Korea, May 2005, Vol.5, pp.3187- 3191.

[8] Hwang J., Shin A. and Yoon H., Dynamic reputation-based incentive mechanism considering heterogeneous networks. In Proc. Of PMMHWWN’08, Vancouver, Canada, October 2008. pp.137-144.

[9] A.Srinivasan, J.Teitelbaum, W.Jie, “DRBTS: Distributed reputation-based beacon trust system”, 2nd IEEE International Symposium on Dependable, Autonomic and Secure Comp. 2006. pp. 277 – 283.

[10] S. Ganeriwal, L.Balzano and M.Srivastava “Reputation-based framework for high integrity sensor networks”, in Proc. SASN’04, Washington, D.C., USA, 2004, pp. 66-77.

[11] N. Ben Salem, J.P. Hubaux, and M. Jakobsson, “Reputation-based wi-fi deployment,” Mobile Computing and Communications Review (MC2R), 2005, vol.9, n.3.

[12] E.C.Efstathiou, P.A.Frangoudis and G.C.Polyzos, “Stimulating Participation in Wireless Community Networks”, in Proc. INFOCOM 2006, Spain, pp.1-13.

[13] T. Moreton and A. Twigg, “Trading in Trust, Tokens, and Stamps”, In Proc. of the 1st Workshop on Economics of P2P Systems, 2003.

[14] A.A.Selcuk, E.Uzun, M.R.Pariente,”A reputation-based trust management system for P2P networks,"Proc. CCGrid'04, pp.251-258

[15] E. Damiani, D. C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante. “Reputation-based approach for choosing reliable resources in peer-to-peer networks”. In Proc..of ACM CCS 2002. pp.207-216.

[16] Li Xiong and Link Liu. “PeerTrust: Supporting Reputation-ased Trust for Peer-to-Peer Electronic Communities”, IEEE transactions on knowledge and data engineering, vol.16, No.7,July 2004.

[17] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, “Karma: a secure economic framework for p2p resource sharing,” In Proc. of 1st Workshop on Economics of P2P Systems, Berkeley, CA, 2003.

[18] F.Doetzer, L.Fischer & P.Magiera, VARS: A Vehicular Ad-Hoc Network Reputation System, in Proc.of WoWMoM’05, pp.454-456.

[19] Ibrohimovna M. and Heemstra de Groot S.M., “Policy-based hybrid approach to service provisioning in federations of personal networks”, in Proceedings of UBICOMM’09, Malta, 2009.

[20] Radu Jurca and Boi Faltings, Using CHI-scores to reward honest feedback from repeated interactions, in Proc.5th Conf. on Autonomous agents and multiagent systems, Hakodate, Japan, 2006, ISBN:1-59593-303-4. pp. 1233-1240.

[21] Radu Jurca and Boi Faltings, Reputation-based Service Level Agreements for Web Services. In ICSOC 2005, vol.3826 pp.396-409.

[22] Reznik P., Zeckhouser R., Friedman E. and Kuwabara K. Reputation systems. Communications of the ACM 43(12), 2000.