Path Optimization and Trusted Routing in MANET: *An Interplay Between Ordered Semirings*

Kiran K. Somasundaram and John S. Baras ⋆

Insitute for Systems Research and Department of Electrical and Computer Engineering
University of Maryland,
College Park, MD 20742
kirans@umd.edu,baras@umd.edu

Abstract. In this paper, we formulate the problem of trusted routing as a transaction of services over a complex networked environment. We present definitions from service-oriented environments that unambiguously capture the difference between trust and reputation relations. We show that the trustworthiness metrics associated with these relations have a linear order embedded in them. Identifying this order structure permits us to treat the trusted routing problem as a bi-objective path optimization problem. We consider bottleneck trust and present polynomial time algorithms to obtain the optimal routing paths in various bi-objective settings. In developing these algorithms, we identify an interesting decomposition principle for $(\min, +)$ and $(\min, \max)$ semirings, which yields a distributed solution.
Keywords-Pareto Optimality, Lexicographic Optimality, Max-Order Optimality, Semirings.

1 Introduction

Mobile Ad Hoc Networks (MANETs) have been envisioned as self-organising networks requiring little or no pre-established infrastructure. The proposed ability of the hosts to dynamically associate themselves with the network in an ad-hoc manner has fuelled a number of application ideas for these networks. However, recent research ([1], [2]) has revealed that this flexibility bears with it several security and survivability threats.

In this paper, we address the problem of trusted routing in MANETs. The lack of pre-installed trust relations in MANETs has steered the networking community to adopt mechanisms from reputation technology for trusted routing ([3],[4], [5]). However, there has been many inconsistencies in defining these trust

⋆ This material is based upon work supported by the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011 and the MURI Award Agreement W911-NF-0710287 from the Army Research Office.

concepts ([1]). Therefore, we introduce precise definitions of trust concepts from the literature on reputation systems, which has been well established and applied in e-services and e-businesses [6].

In this paper, we consider an additive performance metric and a bottleneck trust metric. We show that the trustworthiness metrics used in the literature have a linear order embedded in them. Such order structures are fundamental to optimization ([7]) and help formulate the performance-trust routing problem as a bi-objective optimization problem. We also present distributed polynomial time algorithms which can solve these problems. Our methods find efficient trade-off points between performance and trust for routing. For a more detailed version, see our technical report [8].

The two main contribution of this paper are the following: modeling the performance-trust problem as a bi-objective problem, and providing distributed solutions to the corresponding $(\min, +)$ and $(\min, \max)$ semiring problems.

This paper is organized as follows. In Section 2, we introduce trust and reputation concepts and their application to MANET routing protocols. In Section 3, we present an order-theoretic modeling of trustworthiness metrics. We then develop path metrics for routing in Section 4. Finally, in Section 5, we use the metrics to formulate several bi-objective optimization problems and present algorithms to solve them.

2 Trust and Reputation Inspired Routing Paradigm

Several reputation schemes that mitigate the selfish behaviour in MANET were proposed (e.g., [9], [3],[10], [4]). The concepts of trust and reputation have been developed and applied in diverse areas such as social sciences, e-business and computer science, which resulted in many inconsistent definitions. It has been observed that there is no formal definition of trust and reputation in communication networking literature ([1]). In this paper, we adopt definitions from the literature on *service-oriented environments* because we find a clear distinction between the trust and the reputation concepts. We introduce these concepts in the forthcoming subsections. A detailed introduction is available in our technical report [8].

2.1 Trust and Reputation Concepts

Most trust relations are between a *trusting agent* and a *trusted agent*. Every trust relation involves a *context* C and *time* t. Such a binary relation is called a *direct trust relation*. However, in some scenarios it is not possible for a trusting agent to initiate a direct trust relation with the trusted agent due to spatial or temporal limitations. In such scenarios, the trusting agent requests for recommendations from a third party. The recommendations from this third party about the trusted agent forms the initial trust for bootstrapping the transactions. Such a ternary trust relation, is called a *indirect trust* or *reputation* relation. Associated with every trust relation (direct or indirect) is a trustworthiness measure which captures the strength of a trust relation. We show in Section 3, that these trustworthiness metrics live in an ordered space. This order captures the strength of the trust relations (direct trust, opinion credibility, etc.). To illustrate these relations in a MANET setting, consider any reputation based routing scheme such as *CONFIDANT* ([9]) or *LARS* ([5]). In these protocols, every station performs *self-policing*: trust monitoring, trustworthiness update, and response routing. In this setting, the context of relation is *C=Packet Forwarding*. However, not all trust contexts are restricted *Packet Forwarding*, e.g., the context can be *C=Strength of the Encryption Key*.

2.2 Trust and Reputation in Self-Organised Networks

Reputation systems have already proven useful in e-businesses and e-services [6]. These systems, such as Amazon and eBay, have a centralized architecture for the reputation system where the decision makers are usually humans who look at the trustworthiness metrics and make decisions. However, in self-organized networks, the decision making must be automated [1]. The automated decision making component must be capable of interpreting the trustworthiness metrics.

This decision making component is called the *response routing* component in MANET routing ([11]). A trust-aware routing component should provide two services:

1. Exploit the trusted paths for routing traffic, i.e., for paths which have unambiguous trustworthiness metrics, the decision maker should route traffic without any subjective judgement.
2. Penalize the stations which do not conform to the packet forwarding protocol.

In this paper, we consider only the former as an objective for trusted routing.

3 Trustworthiness and Orders

In this section, we show that most trustworthiness metrics defined in literature form an *ordered set* and in particular they contain a linearly ordered subset that we can exploit for the routing protocols. In this paper we work with trustworthiness metrics which live in a finite set. Such metrics encompass a large body of literature on trust and reputation systems ([12], [13],[14], [15],[16], Amazon, eBay, etc). Again, for detailed definitions of linear orders and their relations to trustworthiness metrics, see [8].

4 Routing Metrics

Most of the works on routing inspired from trust and reputation mechanisms use only the trustworthiness measure to find the optimal routes for packet forwarding ([3], [4], [5]). In all the mechanisms, the trust context *C=Packet Forwarding*. In MANETs, such an approach might route packets through high delay (length) paths. In many scenarios, such high lengths might be intolerable for the application traffic. In this paper, we define two semiring metrics for the path to capture the length and the trustworthiness of a path. We address this problem as a *bi-objective* graph optimization problem.

4.1 Trustworthiness of a Path

Let us consider a path $p = S \rightarrow i_1 \rightarrow i_2 \rightarrow \cdots i_{n-1} \rightarrow T$ in G_c. Associated with every directed arc (i_m, i_n) is a trustworthiness $x(i_m, i_n) \in \mathcal{X}$. In defining the trustworthiness of a path, it is reasonable to adhere to the adage that the strength of a chain (path) is limited to the strength of its weakest link. This is called as bottle-neck trust. If the trustworthiness of a link along a path is unknown, the trustworthiness of this path is also unknown. Since the routing controller works only on the exploitable paths, it suffices to consider paths containing only links whose trustworthiness is exploitable. Let us denote these paths as $\mathcal{P}^L_{ST} = \{p \in \mathcal{P}_{S,T} : \forall (i_m, i_n) \in p, x(i_m, i_n) \in \mathcal{X}^L\}$. Then the trustworthiness of path $p \in \mathcal{P}^L_{S,T}$ is

$$x_p \leq x(i_m, i_n), \forall (i_m, i_n) \in p$$
$$\Rightarrow x_p \leq \min_{(i_m,i_n)\in p} x(i_m, i_n)$$

We use this upper bound as the trustworthiness of the path: $x_p = \min_{(i_m,i_n)\in p} x(i_m, i_n)$. This metric is called the bottleneck trust. Note, the trust in the context *C=Packet Forwarding* cannot be modeled as bottleneck trust. In this context, the trust metric is multiplicative along a path. The bottleneck trust is applicable in contexts such as *C=Strength of the Encryption Keys*.

The duality principle of ordered sets provides an equivalent metric in terms of the dual ordered set. If we impose the dual order on $\mathcal{X}$, the order relation on $\mathcal{X}^\partial$ induces an equivalent dual trust metric

$$x^\partial_p = \max_{(i_m,i_n)\in p} x^\partial(i_m, i_n)$$

4.2 Length of a Path

For legacy routing schemes such as ARPANET ([17]) or IP ([18]), we associate a length l_p for path p. This could be a simple metric such as the hop count or more complicated average delay statistic which captures the delay of the path. In the wireless multi-hop scenario, the delays are primarily due to the congestion in the local MAC. Let us denote the queue congestion metric at station i_m for packets destined to the neighbouring node i_n by $d(i_m, i_n)$. Then,

$$l_p = \sum_{(i_m,i_n)\in p} d(i_m, i_n)$$

The algorithms in this paper are generic and invariant to the path length metric. However, we do assume that the path length composition is an additive composition along the path.

5 Route Selection - A Bi-Objective Optimization Problem

In Subsections 4.1 and 4.2, we introduced the trust and length metrics for the path. A good design criteria for a routing controller is to construct routes that have *high trustworthiness* and *low length*. However, in general these two objectives may be opposing in nature, which results in a trade-off analysis problem. This is the primary object of study in multi-criteria optimization. A summary of the various multi-criteria methods can be found in [19].

The two objectives of the routing controller to constructs routes for a source target pair S, T are: $\{\min_{p \in \mathcal{P}^L_{S,T}} l_p, \max_{p \in \mathcal{P}^L_{S,T}} x_p\}$. The dual trustworthiness transforms the problem into a bi-metric minimization problem: $\{\min_{p \in \mathcal{P}^L_{S,T}} l_p, \min_{p \in \mathcal{P}^L_{S,T}} x^\partial_p\}$. This bi-objective optimization problem is represented as a Multi-Criteria Optimization Problem (MCOP) class ([19]):

$$(\mathcal{P}^L_{S,T}, \begin{bmatrix} l_p \\ x^\partial_p \end{bmatrix}, \mathbb{R}^+ \times \mathcal{X}^{L^\partial}, \leq^2) \tag{1}$$

where $\mathcal{P}^L_{S,T}$ is the set of decision alternatives, $\begin{bmatrix} l_p \\ x^\partial_p \end{bmatrix}$ is a vector valued objective function that maps the decision alternatives to the *length-dual-trust* $(\mathbb{R}^+ \times \mathcal{X}^{L^\partial})$ objective space. There are various $\leq^2$ orders that can be considered for vectors. Table 1 shows the most commonly used orders for two-dimensional vectors $\underline{x}$ and $\underline{y}$. Among these orders, the *Max order* is valid only when $\mathcal{X}^{L^\partial}$ is comparable with $\mathbb{R}^+$.

Notation	Definition	Name
$\underline{x} < \underline{y}$	$x_i \leq y_i \quad i = 1, 2$ and $\underline{x} \neq \underline{y}$	Componentwise
$\underline{x} \leq_{lex} \underline{y}$	$x_k < y_k \quad or \quad \underline{x} = \underline{y} \quad k = \min\{i : x_i \neq y_i\}$	Lexicographic
$\underline{x} \leq_{MO} \underline{y}$	$\max\{x_1, x_2\} \leq \max\{y_1, y_2\}$	Max-order

Table 1: Table of Orders

5.1 Length and Trust Semirings

The presented *MCOP* involves two semiring structures ([20]). The length optimization problem corresponds to a $(\mathbb{R}^+, \min, +)$ semiring. The trust optimization problem corresponds to a $(X^l, \max, \min)$ semiring. Both of these semiring structures have been independently studied and extensively used in the optimization community ([20]). In the theory of MCOP classes, there are many possible methods to combine objectives to obtain solutions ([19]). However, to the best of our knowledge, no theory has combined these two semirings in the various MCOP settings. In the forthcoming subsections, we present distributed polynomial-time algorithms to solve the various bi-objective optimization formulations.

5.2 Pareto Optimal Routing Strategy

The Pareto class for the bi-objective optimization problem is given by

$$(\mathcal{P}^L_{S,T}, \begin{bmatrix} l_p \\ x^\partial_p \end{bmatrix}, \mathbb{R}^+ \times \mathcal{X}^{L\,\partial}, <) \tag{2}$$

where $<$ is the component-wise order defined in Table 1. A path $p^{efficient} \in \mathcal{P}^L_{S,T}$ is Pareto optimal if there exists no path $p \in \mathcal{P}^L_{S,T}$ and $p \neq p^{efficient}$ such that $\begin{bmatrix} l_p \\ x^\partial_p \end{bmatrix} < \begin{bmatrix} l_{p^{efficient}} \\ x^\partial_{p^{efficient}} \end{bmatrix}$. For a general decision problem, there are many *Pareto efficient points* ([19]). One of the common methods to compute efficient points is using the *Haimes-ϵ constraint* method ([21], [22]), which converts all but one of the objectives into constraints and solves the single-objective constraint optimization problem. By considering various relaxations of the Haimes method, we obtain all the Pareto solutions.

Semiring Decomposition: In our case, we show that the Haimes-ϵ constraint method lends itself to a natural decomposition which separates the length and trust semiring. The Haimes formulation is:

$$\min_{p \in \mathcal{P}^L_{S,T}} l_p$$

$$x^\partial_p \leq \epsilon, \quad \epsilon \in \mathcal{X}^{\partial L}$$

$$\text{The constraint } x^\partial_p \leq \epsilon \Rightarrow \max_{(i_m,i_n) \in p} x^\partial(i_m, i_n) \leq \epsilon$$

$$\Rightarrow x^\partial(i_m, i_n) \leq \epsilon, \forall (i_m, i_n) \in p.$$

This implication gives the following decomposition.
Subproblem 1(ϵ): Find a subset of paths in $\mathcal{P}^L_{S,T}$ whose paths have a trustworthiness less than ϵ. This corresponds to finding a pruned subset:

$$\mathcal{P}^{L\text{-}Pruned\text{-}\epsilon}_{S,T} = \{p \in \mathcal{P}^L_{S,T} : x^\partial(i_m, i_n) \leq \epsilon, \forall (i_m, i_n) \in p\}$$

Subproblem 2(ϵ):

$$\min_{p \in P^{L\text{-}Pruned\text{-}\epsilon}_{S,T}} l_p$$

The decomposition is evident as *Subprob* 1(ϵ) involves only the trust semiring and *Subprob* 2(ϵ) involves only the length semiring. This decomposition yields an *edge exclusion* and *shortest path* procedure to solve Eqn. (2). Algorithm 1 builds on these ideas to obtain all the Pareto efficient paths between a source destination pair S, T. It runs on every $i \in V$ and requires only local neighbourhood information ($\mathcal{N}_i$). The routine call `Covered Element(`x`)` returns the covered element of x. The proofs of convergence and correctness are available in our technical report [8].

Algorithm 1 Compute All Pareto Paths

$\mathcal{P}_{S,T}^{L\text{-}Frontier} \leftarrow \emptyset$
$\epsilon \leftarrow \top$
repeat
  $E_r \leftarrow E_c$
  for $j \in \mathcal{N}_i$ **do**
    if $x(i,j) > \epsilon$ **then**
      $E_r \leftarrow E_r \backslash \{(i,j)\}$
    end if
  end for
  $G_r \leftarrow G_r(V, E_r)$
  $\mathcal{P}_{S,T}^{L\text{-}Pruned\text{-}\epsilon} \leftarrow$ Set of paths betweenS, T pair in $G_r(V, E_r)$
  $\mathcal{P}^{candidate}(\epsilon) \leftarrow arg \min_{p \in \mathcal{P}_{S,T}^{L\text{-}Pruned\text{-}\epsilon}} l_p$
  $p^{efficient} \leftarrow arg \min_{p \in \mathcal{P}^{candidate}} x_p^{\partial}$
  $\mathcal{P}_{S,T}^{L\text{-}Frontier} \leftarrow \mathcal{P}_{S,T}^{L\text{-}Frontier} \cup p^{effecient}$
  $\epsilon \leftarrow$ `Covered element`$(x_{p^{efficient}}^{\partial})$
until $\mathcal{P}_{S,T}^{L\text{-}Pruned\text{-}\epsilon} \neq \emptyset$
return $\mathcal{P}_{S,T}^{L\text{-}Frontier}$

5.3 Biased Routing Strategy

A shortcoming of using the Pareto optimality approach is that the number of paths optimal in the Pareto sense is large. One popular approach to prune the Pareto set is *Lexicographic Ordering* ([19]). This method assumes that one metric is superior to other and tries to optimize with respect to the superior metric. Only if two or more feasible solutions are equally optimal in the superior measure, the other measure is considered. This *MCOP* class is represented as $(\mathcal{P}_{S,T}^{L}, \begin{bmatrix} l_p \\ x_p^{\partial} \end{bmatrix}, \mathbb{R}^+ \times \mathcal{X}^{L^{\partial}}, \leq_{lex})$

Based on the lexicographic ordering that we choose, we obtain length or trust biased routing strategies. The strategies consider length or trust as the superior metric respectively. To obtain these paths, we introduce two semiring algebras.

Length-Lexicographic Semiring: $(\mathbb{R}^+ \times \mathcal{X}^{L^{\partial}}, \oplus_d, \otimes)$. The semiring operations are defined as follows. For $(d1, x1^{\partial}), (d2, x2^{\partial}) \in (\mathbb{R}^+ \times \mathcal{X}^{L^{\partial}})$ we define:

$$(d1, x1^{\partial}) \oplus_l (d2, x2^{\partial}) = \begin{cases} (d1, x1^{\partial}) & \text{if} \quad d1 < d2 \\ (d2, x2^{\partial}) & \text{if} \quad d2 < d1 \\ (d1, \min(x1^{\partial}, x2^{\partial}) & \text{if} \quad d1 = d2 \end{cases}$$

$$(d1, x1^{\partial}) \otimes (d2, x2^{\partial}) = (d1 + d2, \min(x1^{\partial}, x2^{\partial}))$$

Trust-Lexicographic Semiring: $(\mathbb{R}^+ \times \mathcal{X}^{L^{\partial}}, \oplus_x, \otimes)$. The semiring operations are defined as follows. For $(d1, x1^{\partial}), (d2, x2^{\partial}) \in (\mathbb{R}^+ \times \mathcal{X}^{L^{\partial}})$ we define:

$$(d1, x1^\partial) \oplus_x (d2, x2^\partial) = \begin{cases} (d1, x1^\partial) & \text{if} \quad x1^\partial < x2^\partial \\ (d2, x2^\partial) & \text{if} \quad x2^\partial < x1^\partial \\ (\min(d1, d2), x1^\partial) & \text{if} \quad x1^\partial = x2^\partial \end{cases}$$

$$(d1, x1^\partial) \otimes (d2, x2^\partial) = (d1 + d2, \min(x1^\partial, x2^\partial))$$

Defining these semirings facilitates the development of a generic distributed algorithm (i.e., Algorithm 2) to obtain lexicographic optimal paths between the source target pair S, T. Again, the algorithm runs at every $i \in V$ and needs only local information. The stations locally store and exchange a dynamic pair $(l, x^\partial)[T]_i^n \in (\mathbb{R}^+ \times \mathcal{X}^{L^\partial})$ which represents the cost of the best lexicographic path from i to T that the algorithm can construct in n iterations.

Algorithm 2 Compute Lexicographic/Biased Path

repeat

$(l, x^\partial)[T]_i^{n+1} = \bigoplus_{k \in \mathcal{N}_i^+} (d_{i,k}, x^\partial(i,k)) \otimes (l, x^\partial)[T]_k^n$

until $(l, x^\partial)[T]_i^n$ converges

The $\bigoplus$ used in Algorithm 2 is $\oplus_l$ and $\oplus_x$ for length and trust biased routing, respectively. We omit the Proof of Lexicographic Optimality of Algorithm 2 due to space limitations; the proof is presented in our technical report [8].

5.4 Conservative Routing Strategy

Another formulation in bi-objective optimization is the *Max-Ordering* (MO) method ([19]). However, this method is applicable to our problem only if the trust values and the path lengths are comparable. If they are, then we obtain a conservative routing strategy. This belongs to the *MCOP* class: $(\mathcal{P}_{S,T}^L, \begin{bmatrix} l_p \\ x_p^\partial \end{bmatrix}, \mathbb{R}^+ \times \mathcal{X}^{L^\partial}, \leq_{MO})$.

The above MCOP class tries to select paths which are optimal in the worst-case sense of trust and delay. Thus it is a conservative strategy for routing, where the cost of the path is governed by the worst-case value of its trust and delay. The problem is stated as

$$\min_{p \in \mathcal{P}_{S,T}^L} \max\{l_p, x_p^\partial\} \tag{3}$$

Semiring Decomposition: The MO problem involves the trust and length semirings. We present decomposition method to separate the semirings. Eqn. (3) can be written as

$$\min_{p \in \mathcal{P}^L_{S,T}} \quad z$$
$$\text{subject to} \quad l_p \leq z$$
$$x^\partial_p \leq z$$

Again, the decomposition yields an *Edge Exclusion* and a *Shortest Path* procedure to obtain the MO paths. This is illustrated in Algorithm 3 which is carried out at every $i \in V$. The algorithm assigns an infinite cost to a non-existent path. The routine `Covering Element(`x`)` returns the covering element of x. The proofs of convergence and optimality are presented in our technical report [8].

Algorithm 3 Compute MO paths

$z \leftarrow \perp$
while True **do**
  $E_r \leftarrow E_c$
  for $j \in \mathcal{N}_i$ **do**
    if $x(i,j) > \epsilon$ **then**
      $E_r \leftarrow E_r \backslash \{(i,j)\}$
    end if
  end for
  $G_r \leftarrow G_r(V, E_r)$
  $\mathcal{P}^{L\text{-}Pruned\text{-}\epsilon}_{S,T} \leftarrow$ Set of paths between(S,T) pair in $G_r(V,E_r)$
  $p^{candidate} \leftarrow arg \min_{p \in \mathcal{P}^{L\text{-}Pruned\text{-}\epsilon}_{S,T}} p$
  if $l_{p^{candidate}} \leq \epsilon$ **then**
    return $p^{candidate}$
  end if
  if $\epsilon =? \top$ **then**
    return No path found
  end if
  $\epsilon \leftarrow$ `Covering Element`(ϵ)
end while

The three algorithms proposed use the `Shortest path` subroutine and `Edge Exclusion` subroutine repeatedly. This is a manifestation of the Semiring decomposition principle. There are many efficient polynomial-time distributed implementations for both of these subroutines ([23]). Thus all these algorithms can be efficiently implemented in a self-organised MANET.

6 Conclusion

In this paper, we present an order-theoretic modeling of the trustworthiness metrics used in different trust and reputation systems. We then treat the trusted routing for a bottleneck trust as a bi-objective path optimization problem involving length and trust metrics. We solve the corresponding Pareto class, which yields the efficient paths. We also solve the Lexicographic and MO classes. In all three cases, we present distributed polynomial-time algorithms that can be implemented in a self-organized MANET.

References

1. S. Buchegger, J. Mundinger, and J.-Y. L. Boudec, "Reputation systems for self-organized networks," *IEEE Technology and Society Magazine*, vol. 27, pp. 41–47, 2008.
2. P. Yau and C. Mitchell, "Security vulnerbilities in ad hoc networks," in *7th International Symposium on Communication theory and applications*, 2003.
3. S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for p2p and mobile ad-hoc networks," in *Proceedings 2nd workshop on the Economics of P2P systems*, 2004.
4. S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," Stanford University, Tech. Rep., 2003.
5. J. Hu and M. Burmester, "Lars: a locally aware reputation system for mobile ad hoc networks," in *44th ACM Annual Southeast regional Conference*, 2006, pp. 119–123.
6. E. Chang, F. Hussain, and T. Dillon, *Trust and Reputation for Service-Oriented Environments: Technologies For Building Business Intelligence And Consumer Confidence*. Wiley, 2006.
7. B. Davey and H. Priestley, *Introduction to lattices and order*. Cambridge University Press, 1990.
8. K. Somasundaram and J. S. Baras, "Path optimization techniques for trusted routing in mobile ad-hoc networks: An interplay between ordered semirings," Institute for Systems Research Technical Report: http://hdl.handle.net/1903/9785, 2008.
9. S. Buchegger and J.-Y. L. Boudec, "Performance analysis of confidant protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks," in *Proceedings MobiHoc*, 2002.
10. ——, "The effect of rumour spreading in reputation systems for mobile ad-hoc networks," in *Proceedings of WiOpt*, 2003.
11. R. Z. P. Resnick, "Trust among strangers in internet transactions: Emperical analysis of ebay's reputation system," *Advances in Applied Microeconomics: The Economics of the Internet and E-Commerce*, vol. 11, pp. 127–157, November 2002.
12. K. Aberer and Z. Despotovic, "Managing trust in a peer-2-peer information system," in *Conference on Information and Knowledge Management. Proceedings of the tenth international conference on Information and knowledge management*, 2001, pp. 310–317.
13. L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer ecommerce communities," in *IEEE Conference on E-Commerce (CEC'03)*, 2003.
14. R. Chen and W. Yeager, "Poblano: A distributed trust model for peer-to-peer networks," Sun Microsystems, Tech. Rep., 2001.
15. A. Rahman and S. Hailes, "A distributed trust model," in *Proceedings of the 1997 workshop on New security paradigms*, 1998.
16. F. Cornelli, E. Damiani, S. D. C. Di, S. Paraboschi, and P. Samarati, "Choosing reputable servants in a p2p network," in *In Proceedings of the 11th World Wide Web Conference*, 2002, pp. 376–386.

17. J. McQuillan, I. Richer, and E. Rosen, “The new routing algorithm for the arpanet,” *IEEE Transactions of Communication*, vol. 28, pp. 711– 719, 1980.
18. G. Malkin, “Rip version 2,” RFC 2453, November 1998, network Working Group. [Online]. Available: http://www.ietf.org/rfc/rfc2453.txt
19. M. Ehrgott, *Multicriteria Optimization.* Springer, 2000.
20. G. Rote, “Path problems in graphs,” in *Computing Supplementum*, vol. 7, 1990, pp. 155–189.
21. Y. Haimes, L. Lasdon, and D. Wismer, “On a bicriterion formulation of the problems of integrated system identification and system optimization,” *IEEE Transactions on Systems,Man and Cybernetics*, vol. 1, pp. 296–297, 1971.
22. V. Chankong and Y. Haimes, *Multiobjective Decision Making: Theory and Methodology.* Elsevier Science Publishing Co,Inc, 1983.
23. J. Kleinberg and E. Tardos, *Algorithm Design.* Addison Wesley, 2005.