THE INSTITUTE FOR SYSTEMS RESEARCH

ISR TECHNICAL REPORT 2010-2

Path Optimization Techniques for Trusted Routing in Mobile Ad-Hoc Networks: An Interplay Between Ordered Semirings

Kiran Somasundaram, John S. Baras

Path Optimization Techniques for Trusted Routing in Mobile Ad-Hoc Networks: *An Interplay Between Ordered Semirings*

Kiran K. Somasundaram, John S. Baras
Department of Electrical and Computer Engineering
University of Maryland,
College Park, MD 20742
Email: 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 which unambiguously capture the difference between trust and reputation relations. We show that the trustworthiness measures 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. Further, we present polynomial time solutions to obtain the optimal routing paths in various bi-objective settings. In developing these algorithms, we identify an interesting semiring decomposition principle that yields a distributed solution.**

***Keywords*-Pareto Optimality, Lexicographic Optimality, Max-Order Optimality, Semirings.**

I. 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 ([31], [25]) 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 ([32],[30], [12]). However, there has been many inconsistencies in defining these trust concepts ([31]). 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 [5]. We find that this literature clearly distinguishes among the different forms of trust relations and the trustworthiness measures associated with each of them. We identify the existence of similar relations hidden in the existing trusted routing protocols.

Next, we use these trust relations and measures to develop automated decision making algorithms which are sensitive to both performance and trust. We show that the trustworthiness measures used in the literature have a linear order embedded in them. Such order structures are fundamental to optimization ([2]) 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. Finally, we propose an application of our algorithms using a case study. We show that our methods find efficient trade-off points between performance and trust for routing.

This paper is organised as follows. We introduce the routing challenges in MANET in Section II. In Section III, we introduce trust and reputation concepts and their application to MANET routing protocols. In Section IV, we present an order-theoretic modelling of trustworthiness measures. We then develop path metrics for routing in Section V. In Section VI, we use the metrics to develop bi-objective optimization problems and algorithms to solve them. Finally, we present a simple case study using our algorithms in Section VII.

II. Routing in MANETs

The problems of routing in MANETs have been addressed, and various solutions inspired from different disciplines have been proposed. Unlike in traditional information networks like the internet, the packet forwarding in MANETs is not restricted to a certain class of routing stations. Every station in a self-organised MANET acts as a potential relay station. Thus, for the functioning of higher layer protocols, it is of paramount importance that the routing conforms to the agreed protocols of *packet forwarding*.

Early routing protocols, both proactive and reactive, proposed for MANETs ([4], [7], [36]) have been shown to have many security vulnerabilities ([33], [3]). The absence of centralized authorities have made many of the existing security solutions infeasible for MANETs. Several proposed schemes use cryptographic primitives to secure the existing MANET routing protocols ([24], [39], [17], [40]). However, these schemes are limited to detecting tampered packets and fail to detect malicious and selfish behaviour. The latter problem is referred to as *free riding* in [31]. Free riding is a well-studied phenomenon in economics, where selfish agents do not offer service at the promised quality ([26]). Free riding is detrimental to a MANET because the main threat in

establishing communication arises from the fact that the selfish nodes might not forward packets ([21]).

In order to solve the above problem, techniques beyond the scope of traditional cryptography have been proposed. These solutions can be broadly classified into *virtual currency schemes* and *reputation schemes*. A virtual currency called *nuglets* was introduced in [19] to stimulate cooperation in a MANET. Another scheme inspired from the credit market was proposed in [34] to induce nodes to cooperate. In these works, mechanisms were introduced to charge and pay each station involved in the transmission of packets.

In these proposed virtual markets, there is a strong dependence on the use of *tamper-proof* hardware to monitor the market fluctuations. This is a very stringent requirement for autonomous MANETs. As an alternative, schemes based on *trust and reputation technology* have been introduced.

III. Trust and Reputation Inspired Routing Paradigm

Several reputation schemes that mitigate the selfish behaviour in MANET were proposed (e.g., [35], [32],[15], [30]). 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 ([31]). 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. Trust and Reputation Mechanisms in Complex Service-Oriented Environments

Modern networks perform diverse functions from serving communication pipelines to sensing to control. The new paradigm in the field of networking is to design algorithms and protocols for these complex networks. Every station in the network seeks services from other stations in network. Thus the network behaves as a complex environment where *network agents* exchange a wide range of services. In such an environment, fraudulent and incomplete practices might occur, and consequently a serving or a served agent is at loss. In order to provide agents with a sense of security to carry out these transactions and services, the ideas of trust and reputation were introduced in service-oriented environments ([5]).

In cyber and network security, we observe that concepts of *trust* and *security* have been treated synonymously. However trust is a much richer abstraction which can model more complex interactions ([5]). To bring things in context, we provide a brief summary of the trust concepts used in e-services. For a detailed exposition, refer to chapters 2 and 8 of [5].

B. Trust and Reputation Concepts

Definition *Trust* is the belief that the trusting agent has in the trusted agent's willingness and capability to deliver a mutually agreed service in a given context and at a given time.

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*. This is illustrated in Fig. 1.

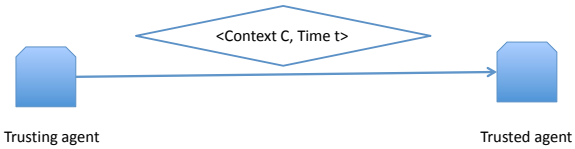

Fig. 1: Direct Trust Relation

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, illustrated in Fig. 2, is called a *indirect trust* or *reputation* relation. In a reputation relation, the trusting agent (X) sends a *reputation query* to a recommending agent (third party Z) requesting for a recommendation for the trusted agent (Y) on a context *C* at time *t*. If Z has a direct trust relation (with the same context *C* at time *t*) with Y, it replies to X with recommendations built from this direct trust relation with Y. This recommendation is accepted by X under another trust relation with a context called *opinion credibility*. This opinion credibility encodes the belief that X has on recommendations from Z. Associated with every trust relation (direct or indirect) is a trustworthiness measure which captures the strength of a trust relation. We show in Section IV, that these trustworthiness measures live in an ordered space. This order captures the strength of the trust relations (direct trust, opinion credibility, etc.).

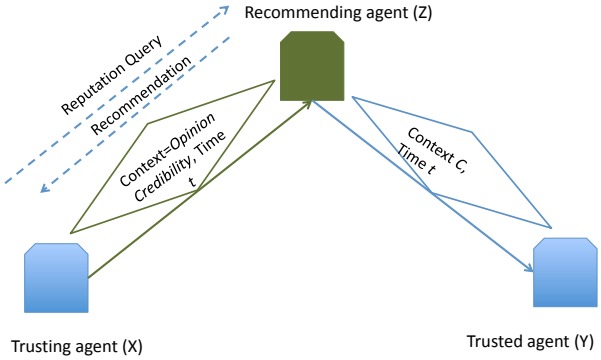

Fig. 2: Indirect Trust Relation

To illustrate these relations in a MANET setting, consider any reputation based routing scheme such as *CONFIDANT* ([35]) or *LARS* ([12]). 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*. The station first establishes a *direct trust relation* with its neighbouring stations by local monitoring. Based on its observations, every station makes trustworthiness updates for every neighbouring station. For stations which it cannot locally monitor, it updates the trustworthiness by requesting for recommendations (via a *indirect trust relation*) from the stations in its local neighbourhood. With reference to the aforementioned relations, we find that a station shares two relations with its local neighbourhood. There is a local direct trust relation (*C=Packet Forwarding*) and an *opinion credibility* relation. In other words, these protocols employ the local neighbourhood as both trusting agents (for packet-forwarding) and recommending agents. Unfortunately, many of the protocols proposed do not clearly distinguish between these two relations in assigning trustworthiness measures. Different trustworthiness measures must be used for the opinion credibility (recommendations) and direct-trust relations ([5]) because a good forwarding agent can be a bad recommender and vice versa.

C. Trustworthiness Measures

In the computer science community, several attempts have been made to define trustworthiness measures, many of which have been born from notions of *subjective probability* ([6]). Recent research suggests that trust measures can also be constructed using the more general *Dempster-Shafer* theory ([23]).

These works suggest different trustworthiness scales. [38] and [16] use a binary trustworthiness measure to encode *trust* and *mistrust*. [20] parametrizes the scale system with various criteria such as agent satisfaction and credibility of the agent feedback. The system proposed in [18] works on normalized trust scale from 0 to 1. [28] proposes a discrete scale system from -1 to 4. [1] proposes an ordinal system with four levels of trustworthiness: {'very trustworthy', 'trustworthy', 'untrustworthy' and 'very untrustworthy'}. There are also other non-numeric systems such as [8] where the rating is based on stars. These schemes are very common in the modern e-business and e-services, e.g., Amazon and eBay.

A famous transitive recommender system is the *web of trust* endorsing in PGP ([27]) in which the endorsed public keys are rated as {unknown, untrusted, marginally trusted, fully trusted}. In this reputation scheme the underlying context of the trust relation is *C=Validity of the key-user binding*.

D. Trust and Reputation Mechanisms in Self-Organised Networks

Reputation systems have already proven useful in e-businesses and e-services [5]. 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 measures and make decisions. However, in self-organized networks, the decision making must be automated [31]. The automated decision making component must be capable of interpreting the trustworthiness measures.

This decision making component is called the *response routing* component in MANET routing ([29]). A trust-aware routing component should:

1) Exploit the trusted paths for routing traffic, i.e., for paths which have unambiguous trustworthiness measures, 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 design routing algorithms which cater to the exploitatory nature of the decision making component. The exploitable paths are those paths which the route decision maker can clearly categorise as trusted or mistrusted. This enables us to provide an optimization approach that is not specific to any particular trustworthiness measure. We generalize the trustworthiness measures using an *order-theoretic* algebra to develop our generic algorithms.

IV. Trustworthiness and Orders

In this section, we show that most trustworthiness measures defined in literature form an *ordered set* and in particular they contain a linearly ordered subset that we can exploit for the routing protocols.

Let us consider a set $\mathcal{X}$. An *order* relation on $\mathcal{X}$ is a binary relation $\leq$ such that $\forall x, y, z \in \mathcal{X}$ satisfies:

i. *Reflexivity* $x \leq x$
ii. *Antisymmetry* $x \leq y$ and $y \leq x \Rightarrow x = y$
iii. *Transitivity* $x \leq y$ and $y \leq z \Rightarrow x \leq z$

The strict order relation $x < y$, for $x, y \in X$ represents $x \leq y$ and $x \neq y$. In a general ordered set not all elements can be compared, i.e., $x||y \Rightarrow x \not\leq y$ and $y \not\leq x$. Here $||$ is the incomparability relation. Another important order relation is the *covering relation* $\prec$. $x \prec y$, if $x < y$ and $x \leq z < y \Rightarrow x = z$. In this case, x is called the *covered element* of y, and y is called the *covering element* of x. A *linearly ordered* set $\mathcal{X}^L$ satisfies an additional *trichotomy* condition: $\forall x, y \in \mathcal{X}^L, x \leq y$ or $y \leq x$.

Another characteristic of ordered set is that they satisfy the *duality principle*: Given an ordered set $\mathcal{X}$, we can construct its dual ordered set $\mathcal{X}^\partial$ by defining $x \leq y$ to hold in $\mathcal{X}^\partial$ *iff* $y \leq x$ in $\mathcal{X}$. $\perp \in \mathcal{X}$ is the *bottom* element if $\perp \leq x, \forall x \in \mathcal{X}$. Dually, the *top* element $\top$ is the bottom element of $\mathcal{X}^\partial$.

To illustrate the order embedding in trustworthiness measures, consider the *PGP* trustworthiness set $\mathcal{X} = \{$unknown (A), untrusted (B), marginally trusted (C), fully trusted $(D)\}$. In trust methods it is incorrect to endow unknown entities with mistrust ([5]). Thus unknown entities form a separate class of agents whose trustworthiness needs to be learned. However the subset $\mathcal{X}^L = \{B, C, D\}$ is the set of measures that can be exploited for routing (see Subsection III-D) because these measures can be clearly classified as trusted or mistrusted. Mathematically, this rationale is represented as:

$$A||x, \quad \forall x \in \mathcal{X}^L$$
$$B \prec C \prec D$$

Clearly, $\mathcal{X}^L$ is a linearly ordered set which can be used for making exploitatory routing decisions. While $\mathcal{X}$ has no bottom element, $\mathcal{X}^L$ has $\perp = B$.

In the paper we work with trustworthiness measures which live in a finite set. Such measures encompass a large body of literature on trust and reputation systems ([16], [20],[28], [1],[8], Amazon, eBay, etc).

Lemma 4.1: Any finite linearly ordered set has a top element.

Lemma 4.2: For any finite linearly ordered set, every element other than $\top$ has a covering element.
The above lemmas are proved in [2].

V. Routing Metrics

Most of the work on routing inspired from trust and reputation mechanisms uses only the trustworthiness measure to find the optimal routes for packet forwarding ([32], [30], [12]). 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.

In ephemeral MANETs, all graph relations, trustworthiness measures and length measures are time varying. In the models we use, although we do not explicitly mention the dependence on time *t*, it is assumed that all the relations and the measures are time varying. We consider a *unit disc* model for communication, which is an abstraction of an isotropic model for radio communication. Let the isotropic communication range of any station be ρ. The unit disc model induces an undirected communication graph $G_c(V, E_c)$ where V is the node set representing the stations in a MANET. Let x_i be the position of the node $i \in V$ in Euclidean space. E_c represents the edge incidence for the communication graph G_c. $(i, j) \in E_c$ *iff* $\parallel x_i - x_j \parallel \leq \rho$. Let $\mathcal{N}_i$ denote the local neighbourhood (the set of one-hop neighbours) for node $i \in V$. The inclusive neighbourhood is given by $\mathcal{N}_i^+ = \mathcal{N}_i \cup \{i\}$. Let $\mathcal{P}_{S,T}$ denote the set of paths between a source-target pair $S, T \in V$.

The trust relations induce a directed graph $G_X(V, A_X)$ called a *trust relation graph*. Here the arc set A_X represents the trust relations. The two different trust relations in the local neighbourhood are shown Fig. 3. We consider an arbitrary context C for these trust relations. Let $dt(i, j)$ denote the direct trust trustworthiness that node i has on j in context C. Let $oc(i, j)$ denote the strength of the opinions (opinion credibility trustworthiness) that i receives from j in context C. Let $r(i, j_m, j_n)$ denote the recommendation that i receives from j_n about j_m in context C. In MANETs, the trust relations for i are not typically limited to $\mathcal{N}_i$ because the mobility of MANET nodes creates dynamic trust relations beyond the local neighbourhood ([23]).

Given the trustworthiness of the trust relations, there exist several fusion rules that fuse these measures to create a trustworthiness for a node (Chapter 10 of [5]). We denote the

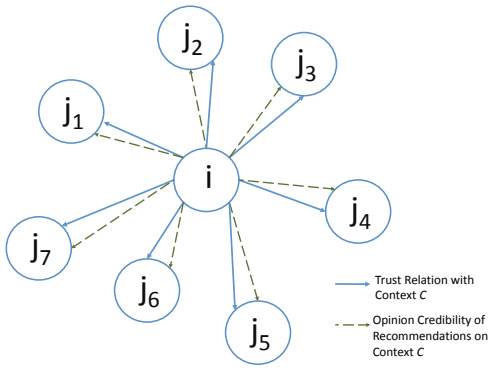

Fig. 3: Local trust relationship

fusion rule at i in rating j by

$$F : (dt(i, j), \{oc(i, j_n), \forall n\}, \{r(i, j, j_n), \forall n\}) \mapsto x$$

The output x of the fusion map F lives in an abstract ordered set $\mathcal{X}$ introduced in Section IV. We assume that this same fusion rule is carried out at every $i \in V$. In essence, the fusion rule associates a trustworthiness $x(i, j), \quad \forall (i, j) \in A_X$.

A. 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. If the trustworthiness of a link along a path falls in an unknown category, 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 this set of paths as

$$\mathcal{P}_{ST}^L = \{p \in \mathcal{P}_{S,T} : \forall (i_m, i_n) \in p, x(i_m, i_n) \in \mathcal{X}^L\}$$

Then the trustworthiness of path $p \in \mathcal{P}_{S,T}^L$ is

$$\begin{aligned} & x_p \leq x(i_m, i_n), \forall (i_m, i_n) \in p \\ \Rightarrow \quad & x_p \leq \min_{(i_m, i_n) \in p} x(i_m, i_n) \end{aligned}$$

We use this upper bound as the trustworthiness of the path.

$$x_p = \min_{(i_m, i_n) \in p} x(i_m, i_n)$$

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

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

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 I: Table of Orders

B. Length of a Path

For legacy routing schemes such as ARPANET ([14]) or IP ([9]), 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 statistics which capture 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.

VI. Route Selection - A Bi-Objective Optimization Problem

In Subsections V-A and V-B, we introduced the trust and length measures 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 [22].

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 ([22]):

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

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 I 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 $\mathbb{R}^+$.

A. Length and Trust Semirings

The presented *MCOP* involves two semiring structures ([10]). 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 ([10]). In the theory of MCOP classes, there are many possible methods to combine objectives to obtain solutions ([22]). 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. We consider the length-dual-trust MCOP in Eqn. 1 as the goal for these algorithms.

B. 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 I. 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* ([22]). One of the common methods to compute efficient points is using the *Haimes-ϵ constraint* method ([41], [37]), 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:

$$\min_{p \in \mathcal{P}^L_{S,T}} l_p \tag{3}$$

$$x^\partial_p \leq \epsilon, \quad \epsilon \in {\mathcal{X}^\partial}^L \tag{4}$$

$$\begin{aligned} \text{The constraint } x^\partial_p \leq \epsilon \quad &\Rightarrow \quad \max_{(i_m, i_n) \in p} x^\partial(i_m, i_n) \leq \epsilon \\ &\Rightarrow \quad x^\partial(i_m, i_n) \leq \epsilon, \forall (i_m, i_n) \in p. \end{aligned}$$

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.

Algorithm 1 Compute All Pareto Paths

$\mathcal{P}_{S,T}^{L\text{-}Frontier} \leftarrow \emptyset$
$\epsilon \leftarrow \top$
repeat
  Construct Reduced Graph $G^r(\epsilon)$ by `Edge Exclusion`
  $E_r \leftarrow E_c$
  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
  $G_r \leftarrow G_r(V, E_r)$

$$\mathcal{P}_{S,T}^{L\text{-}Pruned\text{-}\epsilon} \leftarrow \text{Set of paths between } S,T \text{ pair in } G_r(V,E_r)$$

  `Compute Shortest Path` between S, T on G_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 $\mathcal{P}_{S,T}^{L\text{-}Frontier}$

Proof of Optimality of Algorithm 1: Lemmas 4.1 and 4.2 guarantee the existence of the top and the cover element used in the algorithm. First we show that $\mathcal{P}_{S,T}^{L\text{-}Frontier}$ contains all the Pareto efficient paths in G_c. Suppose $p \in \mathcal{P}_{S,T}^{L\text{-}Frontier}$ is not efficient. This implies that there exists $q \in \mathcal{P}_{S,T}^{L}, q \neq p$ such that $\begin{bmatrix} l_q \\ x_q^{\partial} \end{bmatrix} < \begin{bmatrix} l_p \\ x_p^{\partial} \end{bmatrix}$. Here two cases are possible.

Case I: $l_q < l_p$ and $x_q^{\partial} \leq x_p^{\partial}$.
$x_q^{\partial} \leq x_p^{\partial} \Rightarrow$ if p is preserved during `Edge Exclusion` in Algorithm 1 then so is q. Then `Compute Shortest Path` will never yield p, which is a contradiction.

Case II: $l_q \leq l_p$ and $x_q^{\partial} < x_p^{\partial}$.
Again the `Edge Exclusion` that preserves p also preserves q. If $l_q < l_p$, then p will be sieved out during `Compute Shortest Path`. This implies $l_q = l_p$. Since $p \in \mathcal{P}^{candidate}$, we have $q \in \mathcal{P}^{candidate}$. Then $p^{efficient}$ can never be p as $x_q^{\partial} < x_p^{\partial}$.

Since both cases contradict, we have that p is Pareto efficient. Next we show that there are no more Pareto paths other than those in $\mathcal{P}_{S,T}^{L\text{-}Frontier}$. Suppose $q \notin \mathcal{P}_{S,T}^{L\text{-}Frontier}$ is a Pareto path. Suppose that $\epsilon^1 = \top > \epsilon^2 > \epsilon^3 > \cdots > \epsilon^N$ be the finite sequence of `Edge Exclusion` thresholds. Let $\epsilon^{i+1} < x_q^{\partial} \leq \epsilon^i$ for some i. Consider the iteration when $\epsilon = \epsilon^i$. There are two cases when q is not not chosen in $\mathcal{P}_{S,T}^{L\text{-}Frontier}$.

Case I: $q \notin \mathcal{P}_{S,T}^{candidate}$.
Let $q' = p^{efficient}$ be the efficient path chosen at this iteration. Clearly, $l_{q'} < l_q$. Suppose $x_{q'}^{\partial} \leq x_q^{\partial}$, then $\begin{bmatrix} l_{q'} \\ x_{q'}^{\partial} \end{bmatrix} < \begin{bmatrix} l_q \\ x_q^{\partial} \end{bmatrix}$. This implies that q is dominated by q' and hence is not a Pareto path. This contradiction implies $x_{q'}^{\partial} > x_q^{\partial}$. By definition, `Covered Element` gives $\epsilon^{i+1} \prec x_{q'}^{\partial}$. But $\epsilon^{i+1} < x_q^{\partial} \Rightarrow x_q^{\partial} = x_{q'}^{\partial}$, which is a contradiction.

Case II: $q \in \mathcal{P}_{S,T}^{candidate}$.
Again let $q' = p^{efficient}$ be the efficient path chosen at this iteration. In this case $l_{q'} = l_q$. In this case only q' or q can be Pareto efficient but not both. This is again a contradiction and this completes the reverse implication. Hence $\mathcal{P}_{S,T}^{L\text{-}Frontier}$ contains all the Pareto paths and nothing other than the Pareto paths.

C. 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* ([22]). This method assumes that one measure is superior to the other and tries to optimize with respect to the superior measure. Only if two or more feasible solutions are equally optimal in the superior measure, then 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 the length or the trust as the superior measure, 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.

Proof of Lexicographic Optimality of Algorithm 2: The algorithm converges because all delay weights are non-negative [10]. Consider the length-biased routing. At source S, let p^* be the path returned by the algorithm. Suppose p^* is not an optimal length-biased path. Then $\exists p \neq p^*$ such that:

Case I . $l_p < l_{p^*}$. This is not possible as all the sub-paths are optimal in the length (by definition of $\oplus_l$).

Case II. $l_p = l_{p*}$ and $x_p^{\partial} < x_{p*}^{\partial}$. This is not possible either because the sub-paths are optimal in the trust sense if the lengths are equal (from the definition of $\oplus_l$). A similar proof follows for the trust-biased routing.

D. Conservative Routing Strategy

Another formulation in bi-objective optimization is the *Max-Ordering* (MO) method ([22]). 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

$$\min_{p \in \mathcal{P}_{S,T}^L} \max\{l_p, x_p^{\partial}\} \tag{5}$$

Semiring Decomposition: The MO problem involves the trust and length semirings. We present decomposition method to separate the semirings. Eqn. 5 can be written as

$$\begin{aligned} \min_{p \in \mathcal{P}_{S,T}^L} \quad & z \\ & l_p \leq z \\ & x_p^{\partial} \leq z \end{aligned}$$

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 call `Covering Element`(x) returns the covering element of x.

Algorithm 3 Compute MO paths

$z \leftarrow \perp$
while True **do**
  Construct Reduced Graph $G^r(\epsilon, t)$ by `Edge Exclusion`
  $E_r \leftarrow E_c$
  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
  $G_r \leftarrow G_r(V, E_r)$
  `Compute Shortest Path` between (S, T) on G_r

$$\mathcal{P}_{S,T}^{\textit{L-Pruned-}\epsilon} \leftarrow \text{Set of paths between } (S,T) \text{ pair in } G_r(V, E_r)$$

  $p^{candidate} \leftarrow arg \min_{p \in \mathcal{P}_{S,T}^{\textit{L-Pruned-}\epsilon}} p$
  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

Proof of MO Optimality of Algorithm 3: Since the sequence of ϵ's is monotone and $\mathcal{X}^l$ is finite, the algorithm converges. When the algorithm terminates, $p^{candidate}$ has $l_{p^{candidate}} \leq \epsilon$ and $x_{p^{candidate}}^{\partial} \leq \epsilon$. And $\epsilon \in \mathcal{X}^{\partial}$ is the smallest element for which this condition is satisfied. Thus $p^{candidate}$ upon termination is indeed MO optimal.

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 ([13]). Thus all these algorithms can be efficiently implemented in a self-organised MANET.

VII. Case Study

We present a simple scenario of a MANET that describes the capabilities of the trust methods and the application of our optimization algorithms. Before we discuss the results, we first identify the trust relations hidden in the scenario. Although trust methods can be used to capture complex contexts, we adopt a simple PGP based web of trust model

for ease of illustration. Here the context is *C=Validity of Key-User Binding*. We adopt PGP's trustworthiness measures $\mathcal{X} = \{$*unknown (A), untrusted (B), marginally trusted (C), fully trusted (D)*$\}$. The exploitatory set is $\mathcal{X} = \{B, C, D\}$.

Consider a set of MANET stations (0-22), shown in Fig. 4, which we call a *unit*. The Unmanned Aerial Vehicles (UAVs) X, Y, and Z associate themselves with the unit later. At deployment, all of the unit members' key-user bindings are trusted by all unit members. This means that the *direct trust* graph is a complete directed graph with the trustworthiness measure of each arc being *fully trusted*, i.e., $dt(i_n, i_m) =$ *fully trusted* (D), $\forall i_m, i_n \in \{0, 1, \ldots, 22\}$ and $i_m \neq i_n$. If any non-member k dynamically associates itself to the network, then $\forall i \in \{0, 1, \ldots 22\}$:

$$dt(i,k) = \begin{cases} D & \text{if k can authenticate itself to i.} \\ A & \text{otherwise.} \end{cases}$$

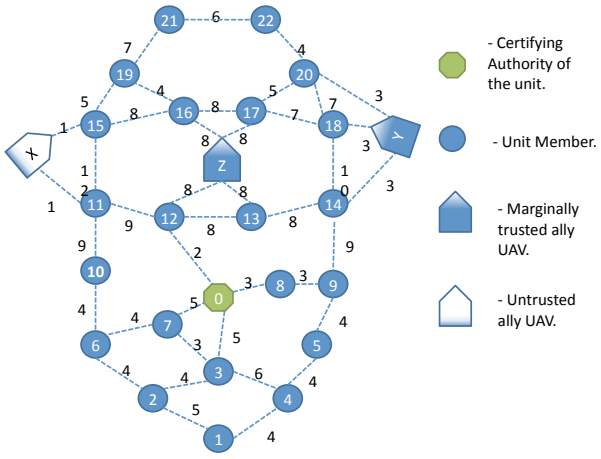

Fig. 4: MANET Scenario with ally UAVs

There is a single certifying authority (node 0, CA), which can endorse other key-user bindings. However, the web of trust endows the other unit members (nodes 1-22) with some endorsing power. We define a simple rule for such a web of trust (OpenPGP offers the freedom for flexible web of trust definitions [27]).

Web of Trust Policy:

1) Any key endorsed by the CA is *fully trusted (D)*.
2) Any key endorsed by three or more fully trusted entities is *marginally trusted (C)*.
3) Any key endorsed by two fully trusted entities is *untrusted (B)*.
4) Any key endorsed by fewer than two entities is *unknown (A)*.

This policy definition assigns the trustworthiness measures for different *opinion credibilities*. We adopt a numeric scheme for the PGP to encode the opinion credibility trustworthiness similar to the one described in [11]. Trustworthiness measures for the opinion credibility are given by:

1) *Member* $\rightarrow$ *CA Relation* = ∞
2) *Member* $\rightarrow$ *Member Relation* = 1
3) *Member* $\rightarrow$ *Non-Member Relation* = 0

The fusion rule between any two entities i and j is then given by

$$F(dt(i,j), \{oc(i,j_n), j_n \in J\}, \{r(i,j,j_n), j_n \in J\}$$
$$= \begin{cases} D & \text{if } dt(i,j)=D \text{ or } \sum_{j_n \in J: r(i,j,j_n)=D} oc(i,j_n)=\infty \\ C & \text{if } dt(i,j) \neq D, \sum_{j_n \in J: r(i,j,j_n)=D} oc(i,j_n) \geq 3 \\ B & \text{if } dt(i,j) \neq D, \sum_{j_n \in J: r(i,j,j_n)=D} oc(i,j_n) = 2 \\ A & \text{if } dt(i,j) \neq D, \sum_{j_n \in J: r(i,j,j_n)=D} oc(i,j_n) < 2 \end{cases}$$

Where J is the set of recommenders. The weights on the edges in Fig. 4 represent the delay in the interface links. We have chosen the example in such a way that links $(11, 15)$ and $(14, 18)$ are overloaded. Let three ally UAVs (i.e., X, Y, and Z) enter the scene to support the traffic for these overloaded links. We assume that at this moment the CA is either offline or is inaccessible to endorse these ally UAVs. However, to sustain the communications, this dynamic association must be endorsed by the unit members. Suppose the ally UAVs are able to authenticate themselves to the neighbouring members, then these members can endorse the UAVs' keys. As per our web of trust fusion F, UAV X becomes *untrusted (B)* and UAVs Y and Z become *marginally trusted (C)*. The fusion rule assigns these trustworthiness measures to every edge in the graph shown in Fig. 4. All edges incident between the unit members are *fully trusted*. The edges incident from UAV X are *untrusted* and those from UAVs Y and Z are *marginally trusted*.

This configuration sets up the problem for our bi-objective routing algorithms. The two measures being the delay and the trust of the paths. Consider a source-target pair $(1, 21)$ for which our distributed algorithm yields all of the Pareto paths (given in Table II). Among the Pareto paths, $p1$ is the delay-lexicographic optimal path and $p3$ is the trust-lexicographic optimal path.

For this instance of the problem, $\mathcal{P}_{1,21}^{\textit{L-Frontier}}$ consists of the paths with all possible trustworthiness measures. The savings in delay by shifting to a path with lower trustworthiness are also computable from $\mathcal{P}_{1,21}^{\textit{L-Frontier}}$. We now introduce a simple change in the scenario which modifies $\mathcal{P}_{1,21}^{\textit{L-Frontier}}$. Suppose that all the interface delays at the UAV Z are changed from 8 to 4, then the frontier reduces to two paths $\{p4, p3\}$, where p_4 is $1 \rightarrow 2 \rightarrow 3 \rightarrow 0 \rightarrow 12 \rightarrow Z \rightarrow 16 \rightarrow 19 \rightarrow 21$ with $(l_{p4}, x_{p4}) = (35,$ *marginally trusted(c)*$)$. This shows that Algorithm 1 is able to identify that all untrusted paths are dominated in the Pareto sense. This suggest that MANET can support efficient minimum-delay traffic by routing through *marginally trusted* and *fully trusted* paths.

However, we cannot consider MO for this example because the trust and delay in this scenario are not comparable. $\mathcal{P}_{S,T}^{\textit{L-Frontier}}$ clearly summarizes the trade-off relations between the trust and the delay measures. This capability of the our distributed algorithms to autonomously compute these tradeoffs enables the system to route different classes of traffic

Path p	$(l_p,\ x_p)$
$p1(1 \to 2 \to 6 \to 10 \to 11 \to X \to 15 \to 19 \to 21)$	(36, B)
$p2(1 \to 4 \to 5 \to 9 \to 14 \to 25 \to 20 \to 22 \to 21)$	(37, C)
$p3(1 \to 2 \to 6 \to 10 \to 11 \to 15 \to 19 \to 21)$	(46, D)

TABLE II: Set of Pareto efficient paths

(based on the sensitivity of the information) through different paths. We trust that this simple scenario captures the order-theoretic modelling of the trustworthiness and the usefulness of our graph optimization algorithms.

VIII. Conclusion

In this paper, we present an order-theoretic modelling of the trustworthiness measures used in different trust and reputation systems. We then treat the trusted routing as a bi-objective path optimization problem involving length and trust measures. 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-organised MANET. We show that this distributed implementation is a manifestation of a Semiring decomposition principle. By means of a case study, we present a simple application of our trusted routing algorithms.

References

[1] Rahman A.A. and Hailes S. A distributed trust model. In *Proceedings of the 1997 workshop on New security paradigms*, 1998.

[2] Davey B.A. and Priestley H.A. *Introduction to lattices and order*. Cambridge University Press, 1990.

[3] Adjih C., Raffo D., and Muhlethaler P. Attacks against olsr: Distributed key management for security. In *2nd OLSR Interop Workshop*, 2005.

[4] Perkins C. Ad hoc on-demand distance vector (aodv) routing. RFC 3561, July 2003.

[5] Dillon T. Chang E., Hussain F. *Trust and Reputation for Service-Oriented Environments: Technologies For Building Business Intelligence And Consumer Confidence*. Wiley, 2006.

[6] Gambetta D. Can we trust trust. In *Trust:Making and Breaking Cooperative Relations*, pages 213–237. Basil Blackwell, 1988.

[7] Johnson D. and Hu Y. The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4. RFC, Feb 2007.

[8] Cornelli F., Damiani E., De Capitani Di S., Paraboschi S., and Samarati P. Choosing reputable servants in a p2p network. In *In Proceedings of the 11th World Wide Web Conference*, pages 376–386, 2002.

[9] Malkin G. Rip version 2. RFC 2453, November 1998. Network Working Group.

[10] Rote G. Path problems in graphs, 1989.

[11] Theodorakopoulos G. and Baras J.S. On trust models and trust evaluation metrics for ad hoc networks. *IEEE Journal on Selected Areas in Communication*, 24(2):318–328, 2006.

[12] Hu J. and Burmester M. Lars: a locally aware reputation system for mobile ad hoc networks. In *44th ACM Annual Southeast regional Conference*, pages 119–123, 2006.

[13] Kleinberg J. and Tardos E. *Algorithm Design*. Addison Wesley, 2005.

[14] McQuillan J., Richer I., and Rosen E. The new routing algorithm for the arpanet. *IEEE Transactions of Communication*, 28:711– 719, 1980.

[15] Buchegger S.m Le Boudec J-Y. The effect of rumour spreading in reputation systems for mobile ad-hoc networks. In *Proceedings of WiOpt*, 2003.

[16] Aberer K. and Despotovic Z. 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*, pages 310–317, 2001.

[17] Sanzgiri K., Dahill B., Levine B.N., Shields C., and Belding-Royer E.M. A secure routing protocol for ad hoc networks. In *Internation conference on Network protocols*, 2002.

[18] Schlosser M. T.m Garcia-Molina H. Kamvar S. D. The eigentrust algorithm for reputation management in p2p networks. In *In Proceedings of the Twelfth International World Wide Web Conference*, pages 640–651, 2003.

[19] Buttyan L. and Hubaux J.-P. Enforced service availability in mobile ad-hoc wans. In *Proceedings MobiHoc*, 2000.

[20] Xiong L. and Liu L. A reputation-based trust model for peer-to-peer ecommerce communities. In *IEEE Conference on E-Commerce (CEC'03)*, 2003.

[21] Conti M., Gregori E., and Maselli G. Cooperation issues in mobile ad hoc networks. In *Internation Workshop on Wireless Ad Hoc Networking*, 2004.

[22] Ehrgott M. *Multicriteria Optimization*. Springer, 2000.

[23] Raya M., Papadimitratos P., Gligor V.D., and Hubaux J.-P. On data-centric trust establishment in ephemeral ad hoc networks. In *INFOCOM*, pages 1238–1246, 2008.

[24] Papadimitratos P. and Haas Z. J. Securing routing for mobile ad hoc networks. In *SCS Communication Networks and Distributed Systems Modelling and Simulation Conference*, 2002.

[25] Yau P. and Mitchell C.J. Security vulnerbilities in ad hoc networks. In *7th International Symposium on Communication theory and applications*, 2003.

[26] Samuelson P.A. The pure theory of public expenditure. *Review of Economics and Statistics*, 36(4):387–389, 1954.

[27] Zimmermann P.R. *The official PGP user's guide*. MIT Press, 1995.

[28] Chen R. and Yeager W. Poblano: A distributed trust model for peer-to-peer networks. Technical report, Sun Microsystems, 2001.

[29] Zechhauser R Resnick P. 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*, 11:127–157, November 2002.

[30] Bansal S. and Baker M. Observation-based cooperation enforcement in ad hoc networks. Technical report, Stanford University, 2003.

[31] Buchegger S., Mundinger J., and Le Boudec J.-Y. Reputation systems for self-organized networks. *IEEE Technology and Society Magazine*, 27:41–47, 2008.

[32] Buchegger S. and Le Boudec J.-Y. A robust reputation system for p2p and mobile ad-hoc networks. In *Proceedings 2nd workshop on the Economics of P2P systems*, 2004.

[33] Marti S., Giuli T.J., Lai K., and Baker M. Mitigating routing misbehaviour in mobile ad hoc networks. In *International conference on Mobile Computing and Networking*, pages 255–265, 2000.

[34] Zhong S., Chen J., and Yang Y.R. A simple cheat proof, credit-based system for mobile ad hoc networks. In *IEEE INFOCOM*, 2003.

[35] Buchegger S.M. and Le Boudec J.-Y. Performance analysis of confidant protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks. In *Proceedings MobiHoc*, 2002.

[36] Clausen T. and Jacquet P. Optimized link state routing protocol (olsr). RFC, Oct 2003.

[37] Chankong V. and Haimes Y.Y. *Multiobjective Decision Making: Theory and Methodology*. Elsevier Science Publishing Co,Inc, 1983.

[38] Wang Y. and Julita V. Bayesian network trust model in peer-to-peer networks. *Lecture notes in computer science*, 2003.

[39] Hu Y.C., Perrig A., and Johnson D.B. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *MOBICOM*, 2002.

[40] Hu Y.C., Johnson D.B., and Perrig A. Sead:secure and effecient distance vector routing for mobile wireless ad hoc networks. In *4th IEEE Workshop on Mobile computing systems and Applications*, 2002.

[41] Haimes Y.Y., Lasdon L.S., and Wismer D.A. On a bicriterion formulation of the problems of integrated system identification and system optimization. *IEEE Transactions on Systems,Man and Cybernetics*, 1:296–297, 1971.