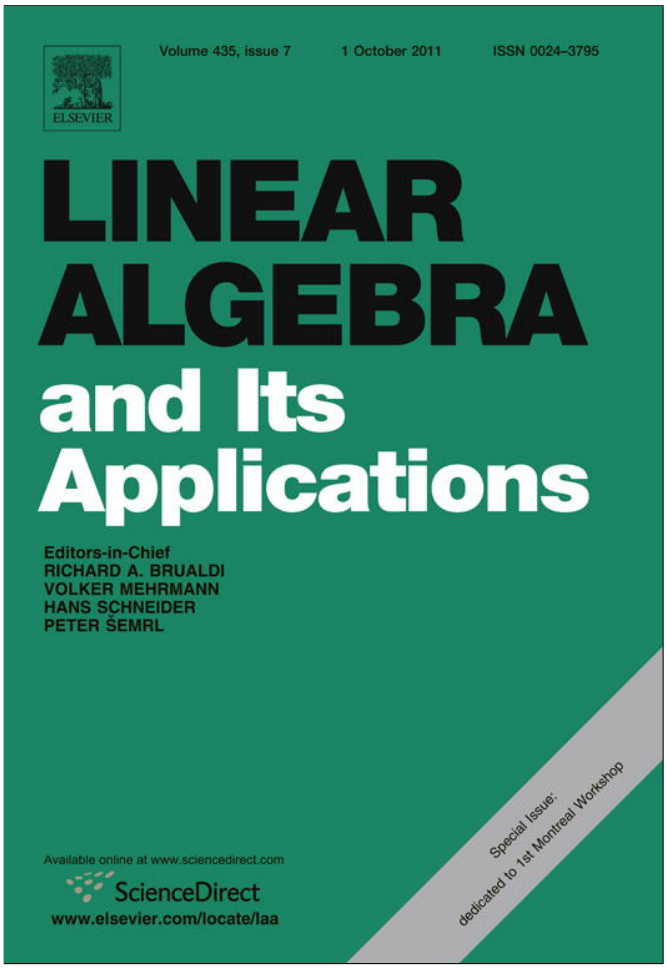

Linear Algebra and its Applications 435 (2011) 1494–1512

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

Solving multi-metric network problems: An interplay between idempotent semiring rules

Kiran K. Somasundaram, John S. Baras *

Department of Electrical and Computer Engineering and The Institute for Systems Research, University of Maryland, College Park, MD 20742, USA

ARTICLE INFO

Article history:
Available online 1 April 2011

Submitted by W. McEneaney

AMS classification:
16
16Y60
90C29

Keywords:
Pareto efficiency
Lexicographic optimality
Max-order optimality
Partial orders
Idempotent semirings
Trusted routing

ABSTRACT

We motivate computations in a multifunctional networked system as instances of algebraic path problems on labeled graphs. We illustrate, using examples, that composition operators used in many function computations in a networked system follow semiring axioms. We present an abstract framework, using a special idempotent semiring algebraic path problem, to handle multiple metrics for composition. We show that using different vector order relations in this abstract framework, we can obtain different rules of compositions such as Pareto, lexicographic and max-order efficiency. Under this framework, we identify a class of tractable composition rules that can be solved in different multi-criteria settings at affordable computational cost. We demonstrate using an example of trusted routing in which logical security rules of admission control can be combined with delay performance metrics in the multi-criteria optimization framework.

1. Introduction

The recent decades have witnessed a paradigm shift in system theory: ubiquity of inexpensive communication and computing devices has spawned several applications that are necessarily distributed among physically separated processors [18,27]. These applications range from distributed databases, transitive security authentication schemes to distributed estimation and control protocols. Since all these applications are built over an underlying communication network, these systems are aptly called *networked systems*. The heterogeneity of devices, which constitute the networked system, and the varied functions that they support have created several interesting problems that did not exist in traditional system theory. For instance, a distributed sensor network is a networked system that

* Corresponding author.
E-mail addresses: kirans@umd.edu (K.K. Somasundaram), baras@umd.edu (J.S. Baras).

0024-3795/$ - see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2011.02.055

performs sensing, control and actuation. To perform this primary functionality, this networked system also supports several communication and security protocols. Further, for these distributed systems, the capabilities and functionalities of the different constituent component subsystems differ significantly. Typically there are different sensor nodes to sense different physical parameters. Certain nodes, which are not energy-limited, might support stronger communication and security mechanisms. In essence, a networked system performs several function computations over a distributed heterogeneous platform. We find that methods from traditional system theory are handicapped to handle this heterogeneity.

Different applications of such a networked system perform computations with different functional metrics. In many cases, the aggregate metric for a particular computation is obtained as composition of local metrics that are measurable by the different constituent subsystems. The rules of composition, to compute this aggregate metric, differ among different computations. For instance, for the routing computation, the metric is typically the interface delay. In this case, the composition of the metrics is additive across the different subsystems. However, for a trust/security computation, a possible metric is the strength of the cryptographic key between a pair of subsystems, and this follows a bottleneck composition. Consequently, for a multifunctional heterogeneous networked system, the different computations can be formulated as a multi-metric network problem with different rules of composition for each of the metrics.

Several computations, such as authentication mechanisms, are specified as logical rules over functional metrics. In these cases, the metric sets are not necessarily totally ordered. We will illustrate with examples from trust evaluation schemes that we need a partially ordered set to describe these metrics. We motivate that for many applications, the composition rules on these metrics follow the semiring axioms.

In the multi-metric setting, the different metrics (for the different computations) are not trivially comparable. For example, metrics such as delay, used in routing, cannot be compared with logical trustworthiness metrics, used in trust evaluation. To handle this, we introduce composition methods from multi-criteria optimization theory [9] that provide tradeoff methods for the different functionalities: different tradeoff methods arise from different vector orders. We develop a common framework where several multi-criteria tradeoff methods can be viewed as instances of idempotent semiring algebraic path problems [17]. Applying different vector-orders to this framework, we show that we can obtain Pareto, lexicographic and max-order solutions. Although the different multi-metric tradeoffs can be encompassed in this idempotent framework, we illustrate, using an example, that these tradeoff methods under some composition rules are computationally intractable. We identify a class of semiring rules that can be solved at affordable computational complexity. The main contributions of this paper are

(1) Exploiting the diversity of idempotent semiring algebra to combine traditional performance metrics such as delay and bandwidth with logical metrics such as trustworthiness.
(2) Identifying a class of composition rules that are computationally tractable in the multi-criteria path problem framework.

This paper is organized as follows. In Section 2, we motivate the need for a multi-metric framework. In Section 3, we introduce semirings and the associated algebraic path problem. We also show that a number of computations can be abstracted by the algebraic path problem. In Section 4, we develop a common framework for multi-metric composition rules inspired from multi-criteria optimization. Finally, in Section 5, we introduce the example of trusted routing. We show that the methods used to solve trusted routing can be extended to a general setting, thereby, identifying a class of tractable multi-metric algebraic path problems.

2. Motivation

Communication networks have grown to become very heterogeneous and multifunctional [27]. Modern wireless multi-hop networks such as Mobile Ad Hoc Networks (MANETs) and wireless sensor

networks have changed the networking paradigm, creating several interesting algorithmic problems that did not exist in traditional networks. Unlike traditional networks, such as the Internet, these networks are deployed to perform a specific functionality, e.g., industrial control. To support this primary functionality, these networked systems perform several other functions, including communication, control and security operations/computations. These functions can be abstracted as optimization or satisfaction problems defined over different metrics that capture the performance of various functionalities of the network, e.g., delay, throughput, security/trust. In many problems, the constraints are specified as rules defined over these metrics [24,3]. Typically, such rules are defined using local metrics, i.e., metrics visible in the local neighborhoods of the different components of the networked system.

To the best of our knowledge, there has been no system model that captures these network problems. We argue that these network problems can be expressed as solutions to problems posed on directed labeled graphs. For these problems, the labels on the nodes and arcs correspond to different metrics, which typically live in partially ordered sets (Section 3.1). In most cases, the problem definition expresses the rules by which these metrics should be composed to obtain aggregate network metrics. We argue that many such rules can be expressed using the operators of a semiring algebra. This is because several well-known composition rules that work with local metrics can be expressed as generalized path problems over semiring algebras [20]. There has been very little work that aims to study the composition of multiple metrics from an algebraic point-of-view. We define a system model that can be used to capture rules with multiple metrics. We show that these rules can be expressed as generalized multi-criteria path problems with an idempotent structure (Section 4).

3. Semiring systems

The most common model used for networked interactions is a labeled directed graph. In this paper, we consider only arc labels. Extending the system model for node labels is simple. In our case, the labels represent the different link metrics.

3.1. Graphs, metrics and orders

Let $G(V, A)$ denote a directed graph, where V is the vertex set of stations or processors and $A \subseteq V \times V$ is the directed arc set. Associated with each arc $(u, v) \in A$ is a label of m metrics, denoted by the vector $\underline{c}_{uv}$. Each component $\underline{c}_{uv}(l) \in S_l,\ \ 1 \leq l \leq m$, where S_l is a partially ordered set. We call S_l the *constituent metric* set and $S = \times_l S_l$ the *product metric* set.

Note that we need the partial order abstraction to encompass logical rules and their corresponding metrics. An example of such a metric is the trustworthiness of a node in an autonomous network. For instance, in the *Pretty Good Privacy* (PGP) certificate signing mechanism [26], the certificates are signed with one of the following trustworthiness levels: *unknown* (a), *untrusted* (b), *marginally trusted* (c) and *fully trusted* (d). Clearly, the unknown level cannot be trivially compared with any of the other levels. To capture these characteristics of metrics used for generic rules, we need a partial order structure.

Consider a set X. A *partial order* relation on X is a binary relation $\leq$ such that $\forall x, y, z \in X$ 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 corresponding *strict order* relation for $x, y \in X$ is

$$x < y \iff x \leq y, \quad x \neq y.$$

In a partially ordered set, not all elements are necessarily comparable, 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*:

$$x \prec y \iff (x < y \quad \text{and} \quad x \leq z < y \Rightarrow x = z).$$

The covering relation $x \prec y$ implies that there exists no other element in between x and y in the ordered set X. In this case, x is called the *covered element* of y, and y is called the *covering element* of x. A *totally ordered* set X satisfies an additional *trichotomy* condition:

$$x, y \in X \Rightarrow x \leq y \quad \text{or} \quad y \leq x.$$

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

For the PGP example, the set $\{b, c, d\}$ forms a totally ordered set with a covering relation $b \prec c \prec d$. And $a||x, \ x \in \{b, c, d\}$. There are no bottom and top elements for this partially ordered set. However, for the totally ordered subset $\{b, c, d\}$, there is a top element d and and a bottom element b. This example is generalized by the following lemmas.

Lemma 3.1. *Any finite totally ordered set has a top element.*

Lemma 3.2. *For any finite totally ordered set, every element other than $\top$ has a covering element.*

The above two lemmas are proved in [8].

In this paper, we provide examples of rules that compose trustworthiness metrics that live in a finite set. Such metrics encompass a large body of the literature on trust and reputation systems ([1,25,6,19,7], Amazon, eBay, etc.).

3.2. Composing metrics

Let P_{ij} denote the set of paths from $i \in V$ to $j \in V$. Note that P_{ii} can include self-loops and always includes the empty path $p = (i)$. For every path $p = (i = u_1, u_2, u_3, \ldots, u_{n-1}, u_n = j) \in P_{ij}$, we obtain the path metric by composing the arc metrics along the path. We obtain an m-dimensional path metric $\underline{w}_p$ by the component-wise composition:

$$\underline{w}_p(l) = \underline{c}_{u_1u_2}(l) \otimes_l \underline{c}_{u_2u_3}(l) \otimes_l \cdots \otimes_l \underline{c}_{u_{n-1}u_n}(l), \quad 1 \leq l \leq m,$$

where $\otimes_l$ is the rule for arc composition of the l^{th} component. For instance, for the metric set $S_l = \{\perp, \top\}$ the arc composition rule $\otimes_l$ could be Boolean disjunction $\vee$ or conjunction $\wedge$. For the more complicated PGP example, it would be any transitive trust evaluation rule [24]. In vector notation, all the compositions are compactly represented as

$$\underline{w}_p = \underline{c}_{u_1u_2} \otimes \underline{c}_{u_2u_3} \otimes \cdots \otimes \underline{c}_{u_{n-1}u_n}. \tag{1}$$

$\underline{w}_p \in S$ is the vector-valued weight of path p. Note that we have not defined the weight of an empty path yet; it will be defined in Section 3.4. Given the weight metrics for all the paths between a pair of vertices, they can be composed to get the *aggregate metric* between the vertices. The composition of the path weights, i.e., *path composition*, is expressed using another operator $\oplus$:

$$x_{ij} = \oplus_{p \in P_{ij}} \underline{w}_p \tag{2}$$

Note that in general x_{ij} need not be of the same type as the vector path weight $\underline{w}_p$. For instance, see the bi-objective shortest path problem in Section 3.4.

The system of equations given by Eqs. (1) and (2) is called the *algebraic path problem*. In general, without any assumed structure on $\otimes$ and $\oplus$, the algebraic path problem is expensive to compute. This is because it involves computing the weights of all the paths between every pair of vertices, which can be exponentially large.

In this paper, we will introduce several rules for path composition used in multi-criteria optimization. We will use the superscript notation to distinguish between the different rules, i.e., for a rule induced by a non-dominance function f, we represent the path composition by $\oplus^f$. For any vector quantity with m elements, say $\underline{y}$, $\underline{y}(q..r), \ 1 \leq q \leq r \leq m$, denotes the sub-vector from index q to r, i.e., $\underline{y}(q..r) = [\underline{y}(q) \ \underline{y}(q+1) \ \ldots \ \underline{y}(r)]^T$.

3.3. Semiring algebra

A semiring is an algebraic structure $(S, \oplus, \otimes)$ that satisfies the following axioms:
(A1) (S,⊕) is a commutative monoid with a neutral element ⓪:

$$a \oplus b = b \oplus a$$

$$a \oplus (b \oplus c) = (a \oplus b) \oplus c$$

$$a \oplus ⓪ = a$$

(A2) (S,⊗) is a monoid with a neutral element ①, *and an absorbing element* ⓪:

$$a \otimes (b \otimes c) = (a \otimes b) \otimes c$$

$$a \otimes ① = ① \otimes a = a$$

$$a \otimes ⓪ = ⓪ \otimes a = ⓪$$

(A3) $\otimes$ *distributes over* $\oplus$:

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

$$(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$$

In the algebraic path problem framework, introduced in Section 3.2, if the path and the arc composition rules correspond to the generalized sum $\oplus$ and the generalized product $\otimes$ of a semiring algebra, the algebraic path problem is called the Semiring Algebraic Path Problem (SAPP). In Section 3.4, we will illustrate that the semiring structure for the algebraic path problem yields a compact representation, which in many cases has reduced computational complexity. For a path composition rule $\oplus$ that follows *A1*, any arc composition rule $\otimes$ that satisfies the axioms *A2* and *A3*, i.e., forms a semiring with $\oplus$, is said to be a *semiring compatible* arc composition for that path composition.

3.4. Semiring algebraic path problems

We argue that a number of composition rules used in networked systems can be expressed over semiring algebras. Many problems of data networking are instances of the SAPP. For example, some of the commonly used semirings in routing are shown in Table 1 [12], where $\hat{\mathbb{Z}}_+ = \mathbb{Z}_+ \cup \{\infty\}$ and $\hat{\mathbb{Z}}_q = \{0, 1, 2, \ldots, q-1, \infty\}$. In [24], the authors show that the rule-based web-of-trust certificate signing in PGP [26] is a special case of a computation over semirings and also construct other semirings for trust evaluation. For examples related to communication networks, we refer to [3]. For more general semiring applications, see [11,10]. In most of these examples, from routing to trust evaluations, the computations correspond to a SAPP [20,24]. To better illustrate this correspondence, we will introduce two example systems before presenting the algebraic framework. The first example is the classical single metric shortest path problem [3] and the second example is the bi-objective/bi-metric shortest path problem. These examples clearly illustrate the difference in the nature of the solutions between

Table 1
Semirings used in network routing.

Name	S	$\oplus$	$\otimes$	⓪	①	Routing application
sp	$\hat{\mathbb{Z}}_+$	min	$+$	∞	0	Shortest path
sp_q	$\hat{\mathbb{Z}}_q$	min	$+$	∞	0	Shortest path (bounded distance)
bw	$\hat{\mathbb{Z}}_+$	max	min	0	∞	Widest path (greatest capacity)
bw_q	$\hat{\mathbb{Z}}_q$	max	min	0	∞	Widest path (greatest bounded capacity)
rel	$[0, 1]$	max	$\times$	0	1	Most reliable path
cup.cap(W)	2^W	$\cup$	$\cap$	$\emptyset$	W	Shared link attributes
cap.cup(W)	2^W	$\cap$	$\cup$	W	$\emptyset$	Share path attributes

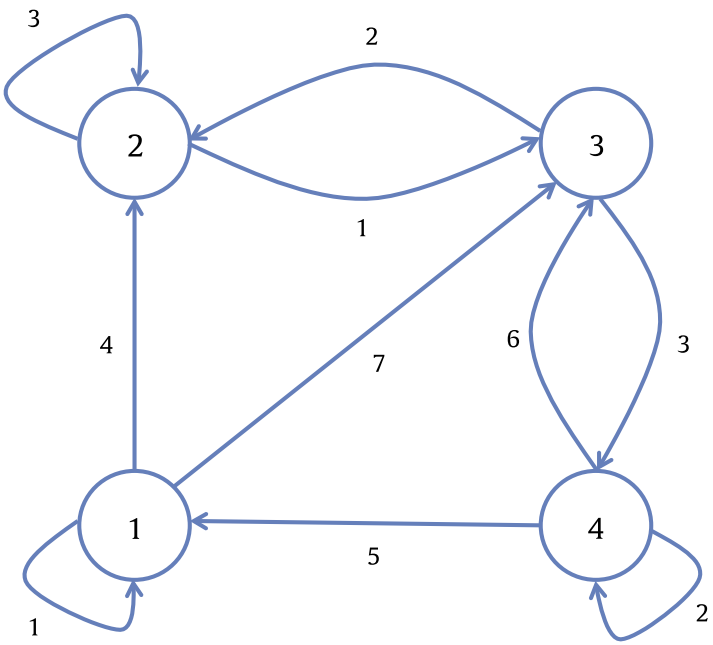

Fig. 1. Example network for shortest path computation.

single-metric and multi-metric network problems: they motivate the need for solution path-sets rather than solution paths for a multi-metric network problem. The examples also serve as introduction to the material in Section 4.

The first example is that of the shortest path computation, which is used in several applications such as data network routing and web mapping. Consider the directed graph shown in Fig. 1 with arc weights denoted by c_{uv}. For this computation, the weight of the path p is given by the rule $w(p) = \sum_{(u,v)\in p} c(u, v)$, and the shortest path weight (aggregate metric) between a pair of vertices i, j is given by the rule $x_{ij} = \min_{p\in P_{ij}} w(p)$. Clearly, the rules of composition can be described by the $(\hat{\mathbb{Z}}_+, \min, +)$ semiring algebra ($\textcircled{0}=\infty$, $\textcircled{1}=0$). Further, these compositions have a structure that can be expressed by a system of equations. Let the weighted adjacency matrix of the graph in Fig. 1 be denoted by

$$\mathbf{C} = \begin{bmatrix} 1 & 4 & 7 & \infty \\ \infty & 3 & 1 & \infty \\ \infty & 2 & \infty & 3 \\ 5 & \infty & 6 & 2 \end{bmatrix}.$$

The artificial weights $\infty = \textcircled{0}$ are used for non-existent arcs. Consider the shortest path from i to j. If $i \neq j$, then this path is of the form $(i = u_0, u_1, \ldots, u_l = j)$. For this shortest path, the sub-path $p' = (u_1, u_2, \ldots, u_l = j)$ must be the shortest path from u_1 to j, and consequently, the shortest path metric is given by $x_{ij} = c_{ik} + x_{kj}$, for $k = u_1$. Thus, the shortest path metric computation for $i \neq j$ can be written as $x_{ij} = \min_{k\in V}(c_{ik} + x_{kj})$. For $i = j$, we also need to consider the empty path from j to j. For the shortest path computation, the weight of an empty path is 0 ($= \textcircled{1}$). Thus, the shortest path computation from j to j can be expressed as $x_{jj} = \min\{\min_{k\in V}(c_{jk} + x_{kj}), 0\}$. For all pairs of vertices, we can express these computations as a system of equations:

$$x_{ij} = \min_{k\in V}(c_{ik} + x_{kj}), \quad \text{for } i \neq j, \quad \text{and}$$
$$x_{jj} = (\min_{k\in V}(c_{jk} + x_{kj})) \min 0,$$

where $(\min_{k\in V}(c_{jk}+x_{kj}))\min 0$ in the above equations is $\min\{(\min_{k\in V}(c_{jk}+x_{kj})), 0\}$. For the example in Fig. 1, the unique solution of shortest path lengths to this system of equations is

$$X = \begin{bmatrix} 0 & 4 & 5 & 8 \\ 9 & 0 & 1 & 4 \\ 8 & 2 & 0 & 3 \\ 5 & 8 & 6 & 0 \end{bmatrix}.$$

Note that for each pair of vertices i and j, the solution corresponds to exactly one path from i to j in G.

The next example is a bi-objective version of the shortest path problem. Consider an example network shown in Fig. 2. It is identical to the network in the previous example, Fig. 1, except for the weights, which are extended to vector weights. In this case, the weight of a path p is given by vector addition $\underline{w}_p = \sum_{(u,v)\in p} \underline{c}_{uv}$. Consider the paths from vertex 1 to vertex 4: path $(1, 3, 4)$ has a weight $[10, 5]^T$ and path $(1, 2, 3, 4)$ has a weight $[8.18]^T$. Each of the paths has a smaller value for one of the two metrics. In such a setting, optimality is usually defined in a Pareto sense [9]. A vector $\underline{v} \in \hat{\mathbb{Z}}_+^2$ is said to be Pareto efficient with respect to a subset $F \subseteq \hat{\mathbb{Z}}_+^2$ if there does not exist in F a vector $\underline{v}' \neq \underline{v}$ that is componentwise smaller than or equal to v. A set of paths is said to be Pareto efficient if its vector weights are Pareto efficient. The Pareto efficient path problem is defined in terms of path-sets rather than paths (Section 6.7 of [11]), and the corresponding Pareto solutions are subsets of $\hat{\mathbb{Z}}_+^2$. For closure, the arc weights need to be in $2^{\hat{\mathbb{Z}}_+^2}$, which is the power-set of $\hat{\mathbb{Z}}_+^2$. For the example in Fig. 2, the weighted adjacency matrix is given by

$$\mathbf{C} = \begin{bmatrix} \{[1,1]^T]\} & \{[4,6]^T\} & \{[7,1]^T\} & \{[\infty,\infty]^T\} \\ \{[\infty\,\infty]^T\} & \{[3,3]^T\} & \{[1,8]^T\} & \{[\infty,\infty]^T\} \\ \{[\infty,\infty]^T\} & \{[2,1]^T\} & \{[\infty,\infty]^T\} & \{[3,4]^T]\} \\ \{[5,6]^T\} & \{[\infty,\infty]^T\} & \{[6,2]^T\} & \{[2,2]^T\} \end{bmatrix}.$$

For the arc composition, we need to define a rule that works on efficient sets (corresponding to Pareto efficient paths). For example, the Pareto efficient paths from vertex 1 to vertex 4 of Fig. 2, i.e., $(1, 3, 4)$ and $(1, 2, 3, 4)$, are composed of the Pareto efficient paths from vertex 1 to vertex 3, i.e., $(1, 3)$ and $(1, 2, 3)$, respectively, and the arc $(3, 4)$. The composition can be expressed using the rule $x_{14} =$

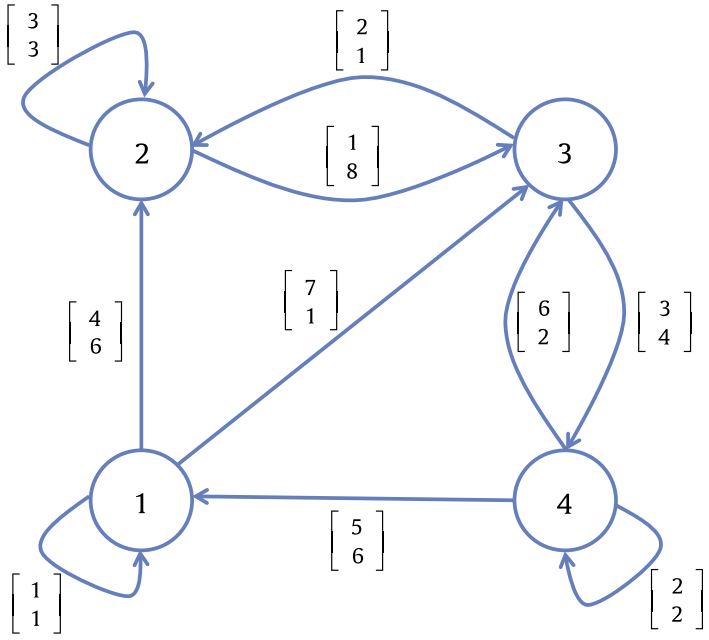

Fig. 2. Example network for bi-objective shortest path computation.

Pareto efficient vectors of the set $\{x_{13} + c_{34}\}$. The path-set composition rule for two path-sets selects all the Pareto efficient vectors in the union of the weights of the two path-sets. Formally, for $X, Y \in 2^{\hat{\mathbb{Z}}_+^2}$, the arc composition rule is

$$X +^P Y = \text{Pareto efficient vectors of the set } X + Y,$$

where $X + Y = \{x + y : x \in X, y \in Y\}$, and the path composition rule is

$$X \text{ Min } Y = \text{Pareto efficient vectors of the set } X \cup Y.$$

(Note that this Min operator is different from the standard min operator for single-metric path problems.)

The Pareto efficient paths are then given by

$$x_{ij} = \text{Min}_{k\in V}(c_{ik} +^P x_{kj}), \text{ for } i \neq j, \text{ and}$$
$$x_{jj} = (\text{Min}_{k\in V}(c_{jk} +^P x_{kj}))\text{Min}\emptyset.$$

Again, the tuple $(2^{\hat{\mathbb{Z}}_+^2}, \text{Min}, +^P)$ forms a semiring with $①=\{[0,0]^T\}$ and $⓪=\emptyset$ (where the Pareto efficient vector of $\emptyset$ is defined to be $[\infty, \infty]^T$).

In the above seemingly different examples, the computations of the aggregate metric over the two different semirings appear to have a common structure: instead of computing the weight of every path, $w(p)$ for all $p \in P_{ij}$ (Eq. (1)) and then computing the aggregate metric by path composition (Eq. (2)), the semiring distribution (Axiom *A3*) factors out the common terms of the computation (of Eqs. (1) and (2)), thereby expressing the aggregate metric in terms of the aggregate metrics of the intermediate vertices. This can be generalized as follows. For a directed graph $G(V, A)$ labeled with elements from an arbitrary semiring $(S, \oplus, \otimes)$ $(c_{uv}, (u, v) \in A)$, artificial arc weights of ⓪ for the non-existent arcs, and empty path weight ①, the generalization of the computation of the above examples is given by

$$x_{ij} = \oplus_{k\in V}(c_{ik} \otimes x_{kj}), \text{ for } i \neq j, \text{ and}$$
$$x_{jj} = (\oplus_{k\in V}(c_{jk} \otimes x_{kj})) \oplus ①. \tag{3}$$

This fixed point equation (Eq. (3)) is called the Semiring Algebraic Path Problem (SAPP). Note that this fixed point equation is a compact representation of the arc and path composition rules (Eqs. (1) and (2)) that follow the semiring axioms.

4. Multi-metric SAPPs

For a multi-metric SAPP, the vector weight of a path is given by the arc composition (Eq. (1)):

$$\underline{w}_p = \underline{c}_{u_1u_2} \otimes \underline{c}_{u_2u_3} \otimes \cdots \otimes \underline{c}_{u_{n-1}u_n}.$$

This corresponds to m different compositions of the form

$$\underline{w}_p(l) = \underline{c}_{u_1u_2}(l) \otimes_l \underline{c}_{u_2u_3}(l) \otimes_l \cdots \otimes_l \underline{c}_{u_{n-1}u_n}(l), \quad 1 \leq l \leq m.$$

Since these compositions follow semiring axioms, each of them corresponds to a monoid $(S_l, \otimes_l)$ with a neutral element $①_l$. The vector arc composition can be represented in the *product monoid* $(S = S_1 \times S_2 \times \cdots \times S_m, \otimes)$. The neutral element of this product monoid is $①= [①_1, ①_2, \ldots, ①_m]^T$. In the path framework, described in Section 3.2, the weight of an empty path is ①.

To define path composition rules for paths with vector weights, we consider rules used in multi-criteria optimization theory [9]. It is known that multi-criteria path problems with additive arc composition in $\mathbb{R}^m$ can be expressed by operators in a special class of semirings with an idempotent structure ([21,16], Section 3.4 of [17], Section 6.7 of [11]).

Table 2
Table of orders and induced laws for $\underline{x}, \underline{y} \in S = \times_{1 \le l \le m} S_l$.

Order Type ($\le$)	Definition	Non-dominance function (f)	Comments
Componentwise, $\underline{x} \le_{com} \underline{y}$	$\underline{x}(i) \le \underline{y}(i) \quad i = 1, 2, \ldots, m$	f^{com}	Partially ordered constituent metric sets induce a partially ordered product metric set
Lexicographic, $\underline{x} \le_{lex} \underline{y}$	$\underline{x}(k) < \underline{y}(k)$ or $\underline{x} = \underline{y}$,where $k = \min\{i : \underline{x}_i \ne \underline{y}_i\}$	f^{lex}	"
Max-order, $\underline{x} \le_{MO} \underline{y}$	$\max\{\underline{x}(1), \underline{x}(2), \ldots, \underline{x}(m)\} \le \max\{\underline{y}(1), \underline{y}(2), \ldots, \underline{y}(m)\}$	f^{MO}	Totally ordered constituent metric sets induce a totally ordered product metric set

4.1. Idempotent semirings

For an idempotent semiring, the $\oplus$ is idempotent:

$$a \oplus a = a, \quad a \in S.$$

It is shown in [11] that this idempotent property induces a canonical (partial) order that is expressed as

$$a \le b \iff a = a \oplus b.$$

(Note that canonically ordered semirings are also called *dioids* in the literature [11].) All the semirings in Table 1 are idempotent semirings. A sub-class of idempotent semirings is called *selective semirings* where the $\oplus$ operator is selective:

$$a \oplus b = a \text{ or } b, \ a, b \in S.$$

For example, sp, sp_q, bw, bw_q and rel of Table 1 are selective semirings. However, cap.cup(W), cup.cap(W) and the bi-objective sp (example in Section 3.4) are idempotent, but not selective.

4.2. Idempotent rules for multi-metric SAPP

For the multi-metric network problems that we consider, the metrics, such as logical trust metrics, live in an arbitrary ordered set (Section 3.1). For these metrics, the arc composition rules are complicated rules such as admission control rules (trusted routing example in Section 5.1). Even in these cases, the methods of [21] can be extended, to handle logical rules, by defining suitable dominance functions.

The metrics that we consider for our systems live in a vector-valued product set ($S = \times_{l=1}^{m} S_l$), where the constituent set S_l is an ordered set. Although the constituent metric sets S_l, $1 \le l \le m$ are partially ordered, there is no natural order induced in the product set. There are several order relations to compare vectors that can be used to define an order on S [9]. Table 2 shows the orders that are most commonly used to compare vectors. We will show that each of these orders induces a different idempotent law for path composition.

Every order relation in Table 2 creates *efficient vectors*. The notion of efficiency is generic to any partially ordered set. We adopt the terminology of efficiency from [9] to our multi-metric path problems. We represent the multi-metric efficiency for the algebraic path problem by the tuple

$$(P_{ij}, \underline{w}, S, \le).$$

The above tuple indicates that the decision set P_{ij} is the set of paths from vertex i to vertex j. The function $\underline{w} : P_{ij} \to S$ maps the decision set P_{ij} to the objective set S. Finally, the order that is used to compare the elements of the objective set, S, is the order relation $\le$. Depending on the type of order used, we obtain different order relations for S (Table 2).

For the order relations defined in Table 2, the *strict order* is defined for $\underline{x}, \underline{y} \in S$ by

$$\underline{x} < \underline{y} \iff \underline{x} \le \underline{y} \quad \text{and} \quad \underline{x} \ne \underline{y}.$$

With this strict order relation, we can define *non-dominated* vectors for any subset $S' \in 2^S$, where 2^S is the power set of S. A vector $\underline{x} \in S'$ is *non-dominated* in S' if there is no other vector $\underline{y} \in S'$ such that $\underline{y} < \underline{x}$. The set of all non-dominated vectors in $S' \in 2^S$ is called the non-dominated frontier of S' and is denoted by $f(S')$. Note that the non-dominated frontier can be defined for any partially ordered set. This non-dominated frontier defines an idempotent law: for any $U, V \in 2^S$,

$$U \oplus^f V = f(U \cup V).$$

We call the above law the *efficiency idempotent* law. The superscript f indicates the non-dominance function, and thereby the order relation used to construct the idempotent law. Clearly, $(2^S, \oplus^f)$ is a commutative monoid with neutral element $\emptyset$.

For the algebraic path problem (Eq. (2)), applying the above idempotent rule for path composition yields *non-dominated* solutions and *efficient* paths: for a pair of vertices $i, j \in V$, the efficiency idempotent law $\oplus^f$ yields the set of all *non-dominated* solutions, denoted by x^f_{ij}, and the corresponding solution path-set called the *efficient path-set*.

The arc composition rule (Eq. (1)) that is semiring compatible with $\oplus^f$ is denoted by $\otimes^f$. As in the case of the bi-objective sp example, the arc composition operates on the sets in 2^S. Here the product/arc composition of two sets follows a non-dominated version of *Minkowski products*:

$$U \otimes^f V = f(\{u \otimes^f v \ : \ u \in U, \ v \in V\})$$

This is another monoid $(2^S, \otimes^f)$. Note that the rules of composition are generalizations of the rules defined for the bi-objective sp problem (Section 3.4). The aggregate metric for efficiency can be expressed in the idempotent semiring $(2^S, \oplus^f, \otimes^f)$ and the composition rules can be represented by the following SAPP, which we call the *efficiency SAPP*.

$$\begin{aligned} x^f_{ij} &= \oplus^f_{k \in V} \left(\{\underline{c}_{ik}\} \otimes^f x^f_{kj} \right), \quad \text{for } i \neq j, \quad \text{and} \\ x^f_{jj} &= \left(\oplus^f_{k \in V} (\{\underline{c}_{jk}\} \otimes^f x^f_{kj}) \right) \oplus^f \{\textcircled{1}\}. \end{aligned} \tag{4}$$

The solutions $x^f_{ij}, \ i, j \in V$, are sets of non-dominated vectors for the non-dominance function f.

The componentwise order induces an efficiency that is called *Pareto efficiency*:

$$(P_{ij}, \underline{w}, S, \leq_{com}).$$

In Pareto efficiency, the componentwise order definition requires that the constituent metric sets be partially ordered, in the least. The resulting product metric set S is again partially ordered. Note that even if the constituent sets are totally ordered, in general, the product set is only partially ordered. The non-dominance function f^{com} yields the idempotent Pareto efficient semiring $(2^S, \oplus^{f^{com}}, \otimes^{f^{com}})$.

The lexicographic order induces an efficiency that we call *lexicographic efficiency*. This differs from the commonly used lexicographic optimality that appears in the literature [9]. We denote the lexicographic efficiency by the tuple.

$$(P_{ij}, \underline{w}, S, \leq_{lex}).$$

Again, the lexicographic order definition requires the constituent metric sets to be partially ordered and induces a product set that is partially ordered. However, if the constituent metric set is totally ordered, then so is the product metric set. In this case, lexicographic efficiency reduces to lexicographic optimality. We represent the idempotent lexicographic efficient semiring by $(2^S, \oplus^{f^{lex}}, \otimes^{f^{lex}})$.

The last efficiency that we consider is the max-order efficiency. It is also referred to as max-order optimality, for reasons which will become obvious. Max-order efficiency is represented by the tuple

$$(P_{ij}, \underline{w}, S, \leq_{MO}).$$

The definition of max-order requires the constituent metric sets S_l, $1 \leq l \leq m$ to be totally ordered, and the product set $S = \times_{1 \leq l \leq m}$ is also totally ordered. This order is useful only if the metrics are

comparable directly, i.e., the different components of the vectors are themselves comparable. The idempotent path composition law becomes selective because of this total order, i.e.,

$$\underline{x} \oplus^{f^{MO}} \underline{y} = \begin{cases} \underline{x} \text{ if } \underline{x} \leq_{MO} \underline{y} \\ \underline{y} \text{ if } \underline{y} \leq_{MO} \underline{x} \end{cases}$$

Depending on the properties of the composition rules $\oplus^f$, $\otimes^f$, the computational complexity of solving the efficiency SAPP differs. Consider the example of the bi-objective/bi-metric sp problem introduced in Section 3.4. It is a two metric problem on a directed graph $G(V, A)$ with each metric in $S_1 = S_2 = \hat{\mathbb{Z}}_+$, and hence, $S = \hat{\mathbb{Z}}_+^2$. The arc composition rule for $[a_1, a_2]^T, [b_1, b_2]^T \in \hat{\mathbb{Z}}_+^2$ is standard vector addition, i.e., $[a_1, a_2]^T + [b_1, b_2]^T = [a_1 + b_1, a_2 + b_2]^T$. The path composition corresponds to finding Pareto efficient solutions. Thus, this problem can be expressed as a SAPP in $(2^{\hat{\mathbb{Z}}_+^2}, \oplus^{f^{com}}, +^P)$. It is shown in Chapter 9 of [9] that the bi-metric shortest path problem can be reduced to a Knapsack problem, showing that the problem is NP complete. In essence, this means that the problem is computationally hard to solve. Thus as this example illustrates, even a simple arc composition rule such as vector addition can make the problem intractable. In the next section, we identify a class of arc composition rules that can be solved for efficiency at affordable computational cost.

5. A class of tractable multi-metric SAPPs

Let one constituent monoid, say without loss of generality $(S_1, \otimes_1)$, be a partially ordered monoid. This means that there is an order relation $\leq$ that is compatible with the internal law $\otimes_1$:

$$a, b, c \in S_1, \quad a \leq b \Rightarrow a \otimes_1 c \leq b \otimes_1 c.$$

For $S_1' \in 2^{S_1}$, an element $a \in S_1'$ is non-dominated in S' if there exists no other $b \in S_1'$ such that $b < a$. We can define the non-dominance function Min (corresponding to the partial order in the constituent set S_1):

$$S_1' \in 2^{S_1}, \ \text{Min}(S_1') = \text{set of non-dominated points in } S_1'.$$

The non-dominance function Min reduces to the minimum function if S_1 is totally ordered. The other constituent monoids, $(S_l, \otimes_l)$ $2 \leq l \leq m$, are selective:

$$a, b \in S_l, \quad a \otimes_l b = a \,(\text{or})\, b, \quad 2 \leq l \leq m.$$

This induces a total order on S_l, $2 \leq l \leq m$. Boolean lattices, $(\hat{\mathbb{Z}}_+, \min)$, $(\hat{\mathbb{Z}}_+, \max)$ are examples of monoid rules that are selective. Since the set is totally ordered, we can define the minimum of two elements of S_l, i.e.,

$$a, b \in S_l, \ \min(a, b) = a \iff a \otimes_l b = a.$$

The product monoid is assumed to be semiring compatible with the idempotent path composition rule. We will show that this product monoid, as constructed, when used for arc composition yields an efficiency SAPP that is solvable for all the different order relations introduced in Section 4. In particular, we will show that for each of the idempotent laws of the path composition, discussed in Section 4, there is a special decomposition principle that decouples the rules $\otimes_l$, $2 \leq l \leq m$ from $\otimes_1$. To better illustrate this decomposition, we visit the Mobile Ad hoc Network (MANET) trusted routing example described in [23,22]. In this example, we develop a bi-metric problem, involving the length (delay) and the dual trustworthiness of paths. We will show that the metrics can be combined in the different multi-criteria settings introduced in Section 4, and we will provide solution methods for the different efficiency SAPPs.

5.1. Trusted routing: an example

We will briefly describe the trusted routing problem in MANETs. Most of the previous works on routing, inspired from trust and reputation mechanisms, use only the trustworthiness value to find optimal routes for packet forwarding [4,2,14]. Such an approach might route packets through high delay (length) paths. In many scenarios, high delays are intolerable for the application traffic. To make the routers sensitive to both delay and trust, we posed the problem as a bi-objective graph optimization problem [22].

In ephemeral MANETs, all graph relations, trustworthiness and length values are time varying. In the models we use, although we do not explicitly mention the dependence on time, it is assumed that all the relations and the values are time varying. The trust relations form a directed labeled graph $G(V, A)$ called a *trust relation graph*. The arc set A represents the trust relations. Let $t(u, v)$ denote trustworthiness value for $(u, v) \in A$. As illustrated in Section 3.1, the trustworthiness value t lives in a partially ordered set. For this example, let us suppose the context corresponds to the strength of the PGP certificate. For routing, we consider only exploitative decisions and not exploratory decisions [22]: route only using nodes whose trustworthiness is discovered and not using the nodes whose trustworthiness is unknown. Consequently, $t \in$ {*untrusted* (b), *marginally trusted* (c) and *fully trusted* (d)}, which is a totally ordered set. In this context, the arc composition is given by *bottleneck trust* [22]: the trust of a path is limited by the minimal trust of any arc on the path. The objective of trusted routing is to select paths with different levels of trust (validity of key-user binding) for different types of traffic. In essence, the path selection in this context is an *admission control* policy that allows or disallows traffic flow along a path.

For the bi-objective trusted routing problem, there are two metrics, the delay and the trustworthiness of arcs. The delay lives in $S_1 = \hat{\mathbb{R}}_+$ and the trustworthiness lives in $S_2 = \{b, c, d\}$. We denote the dual-trustworthiness set by $S_2^\partial = \{b^\partial, c^\partial, d^\partial\}$ (with a covering relation $d^\partial \prec c^\partial \prec b^\partial$) and the dual-trustworthiness of the arcs by $t^\partial(u, v)$. For a path $p = (i = u_1, u_2, u_3, \ldots, u_n = j)$ in G, the delay of a path is the sum of the delays along all arcs:

$$l_p = \sum_{(u,v)\in p} d(u, v), \tag{5}$$

where $d(u, v)$ is the delay of the arc $(u, v) \in A$. The trustworthiness of a path is the strength of its weakest arc:

$$t_p = \min_{(u,v)\in p} t(u, v)$$

It is useful to define the *dual-trustworthiness* of a path:

$$t_p^\partial = \max_{(u,v)\in p} t^\partial(u, v). \tag{6}$$

Note that the notion of dual-trustworthiness is helpful to formulate the trusted routing problem as a bi-metric minimization problem: the problem is to find paths with minimal length and dual-trustworthiness in the multi-criteria setting. Equations (5) and (6) are arc composition laws that can be expressed using monoids $(S_1, +)$ and (S_2, max), respectively. The product monoid of arc composition satisfies the conditions of our construction, introduced in the start of this section: (S_2, max) is selective and induces a total order in S_2.

To study the different tradeoffs of this bi-objective problem, we can pose the trusted routing problem as an efficiency problem (introduced in Section 4) with these arc composition rules:

$$\left(P_{ij}, \begin{bmatrix} l_p \\ t_p^\partial \end{bmatrix}, S_1 \times S_2^\partial, \leq\right)$$

With different order relations (Table 2), we obtain different routing strategies: pareto optimal routing, Biased routing and conservative routing. In the rest of this subsection, we will introduce these efficiency (routing) problems and present algorithms to solve them.

5.1.1. Pareto optimal routing strategy

The Pareto bi-objective efficiency is

$$\left(P_{ij}, \begin{bmatrix} l_p \\ t_p^{\partial} \end{bmatrix}, S_1 \times S_2^{\partial}, \leq_{com}\right).$$

One of the common methods to compute Pareto non-dominated points is using the *Haimes-ϵ constraint* method ([13,5]), which converts all but one of the objectives into constraints and solves the single-objective constraint optimization problem. By sweeping across different constraints, we obtain all the Pareto solutions.

Semiring decomposition: For the trusted routing problem, we show that the Haimes-ϵ constraint method lends itself to a natural decomposition that separates the length and trust monoid rules. The Haimes formulation is:

$$\min_{p \in P_{ij}} l_p \tag{7}$$

$$t_p^{\partial} \leq \epsilon, \quad \epsilon \in S_2^{\partial}. \tag{8}$$

$$\text{The constraint } t_p^{\partial} \leq \epsilon \Rightarrow \max_{(u,v)\in p} t^{\partial}(u,v) \leq \epsilon$$
$$\Rightarrow t^{\partial}(u,v) \leq \epsilon, \forall (u,v) \in p.$$

This implication gives the following decomposition.
Subproblem 1(ϵ): Find the subset of paths in P_{ij} whose arcs have a dual trustworthiness at most ϵ. This corresponds to finding a pruned subset

$$P_{ij}^{\text{Pruned}-\epsilon} = \{p \in P_{ij} : t^{\partial}(u,v) \leq \epsilon, \forall (u,v) \in p\}$$

Subproblem 2(ϵ):

$$\min_{p \in P_{ij}^{Pruned\text{-}\epsilon}} l_p$$

The decomposition is evident because *Subprob* 1(ϵ) involves only the dual trust and *Subprob* 2(ϵ) involves only the path length. We show that *Subprob* 1(ϵ) can solved using a simple *arc-exclusion* algorithm, Algorithm 1.

Algorithm 1 Compute pruned path set $P_{ij}^{\text{Pruned}-\epsilon}$

input: G
Remove all arcs $(u,v) \in A$ in G with $t^{\partial}(u,v) > \epsilon$ to form a reduced graph $G_r(\epsilon)$
$P_{ij}^{\text{Pruned}-\epsilon} \leftarrow$ set of paths between i and j in $G_r(\epsilon)$
return $P_{ij}^{\text{Pruned}-\epsilon}, G_r(\epsilon)$

Proposition 5.1. *The set of paths returned by Algorithm 1, $P_{ij}^{Pruned-\epsilon}$, solves Subprob 1(ϵ).*

Proof. By construction, none of the arcs (u,v) in $G_r(\epsilon)$ have $t^{\partial}(u,v) > \epsilon$. Consequently, all paths have arcs (u,v) whose $t^{\partial}(u,v) \leq \epsilon$. □

Algorithm 2 works on the reduced graph $G_r(\epsilon)$ to obtain all the Pareto efficient paths between a source destination pair i, j: The algorithm runs a shortest path routine on the pruned path set $P^{\text{Pruned}-\epsilon}$ to find weakly Pareto efficient paths $P^{\text{candidate}}$. Then the Pareto efficient path is picked up from this candidate set $P^{\text{candidate}}$. Then the algorithm makes use of the finite structure of S_2 to traverse the non-dominated frontier: It traverses through a sequence of covered elements and terminates when the reduced graph $G_r(\epsilon)$ becomes disconnected. It returns the Pareto efficient paths $P_{ij}^{\text{efficient}}$. In Algorithm 2, *Covered Element(x)* returns the covered element of $x \in S_2^{\partial}$.

Algorithm 2 Compute All Pareto Paths

$P_{ij}^{\text{efficient}} \leftarrow \emptyset$
$\epsilon \leftarrow \top$
repeat
  $P^{\text{candidate}} \leftarrow arg \min_{p \in P_{ij}^{\text{Pruned}-\epsilon}} l_p$
  $p^{\text{efficient}} \leftarrow arg \min_{p \in P^{\text{candidate}}} t_p^{\partial}$
  $P_{ij}^{\text{efficient}} \leftarrow P_{ij}^{\text{efficient}} \cup p^{\text{efficient}}$
  $\epsilon \leftarrow$ *Covered Element*$(t_{p^{\text{efficient}}}^{\partial})$
until $P_{ij}^{\text{Pruned}-\epsilon} \neq \emptyset$
return $P_{ij}^{\text{efficient}}$

Proposition 5.2. *Algorithm 2 returns all the Pareto efficient paths in G.*

Proof. Lemmas 3.1 and 3.2 guarantee the existence of the top and the cover element used in the algorithm. Since S_2^{∂} is finite, the sequence of covers returned by repeated calls of the function *Covered Element* in Algorithm 2 is also finite. Consequently, the algorithm terminates in a finite number of iterations/steps.

First, we show that $\mathcal{P}_{ij}^{\text{efficient}}$ contains only Pareto efficient paths in G. Suppose $p \in P_{ij}^{\text{efficient}}$ is not efficient. This implies that there exists $q \in P_{ij}$, $q \neq p$ such that $\begin{bmatrix} l_q \\ t_q^{\partial} \end{bmatrix} < \begin{bmatrix} l_p \\ t_p^{\partial} \end{bmatrix}$. Here two cases are possible.

Case I: $l_q < l_p$ and $t_q^{\partial} \leq t_p^{\partial}$.

$t_q^{\partial} \leq t_p^{\partial}$ implies that if $p \in P^{\text{Pruned}-\epsilon}$, then $q \in P^{\text{Pruned}-\epsilon}$. If $l_q < l_p$, then $p \notin P^{\text{candidate}}$, which is a contradiction.

Case II: $l_q \leq l_p$ and $t_q^{\partial} < t_p^{\partial}$.

If $p \in P^{\text{Pruned}-\epsilon}$, then $q \in P^{\text{Pruned}-\epsilon}$. If $l_q < l_p$, then $p \notin P^{\text{candidate}}$. This implies $l_q = l_p$. Since $p \in P^{\text{candidate}}$, we have $q \in \mathcal{P}^{\text{candidate}}$. Then $p^{\text{efficient}} \neq p$ because $t_q^{\partial} < t_p^{\partial}$.

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 $P_{ij}^{\text{efficient}}$. Suppose $q \notin P_{ij}^{\text{efficient}}$ is a Pareto path. Suppose that $\epsilon^1 = \top > \epsilon^2 > \epsilon^3 > \cdots > \epsilon^N$ be the finite sequence of ϵ's returned by the *Covered Element* function in Algorithm 2. Let $\epsilon^{k+1} < t_q^{\partial} \leq \epsilon^k$ for some k. Consider the iteration when $\epsilon = \epsilon^k$. There are two cases when q is not chosen in $P_{ij}^{\text{efficient}}$.

Case I: $q \notin P^{\text{candidate}}$.

Let $q' = p^{\text{efficient}}$ be the efficient path chosen at this iteration. Clearly, $l_{q'} < l_q$. Consider the sub-case $t_{q'}^{\partial} \leq t_q^{\partial}$, then $\begin{bmatrix} l_{q'} \\ t_{q'}^{\partial} \end{bmatrix} < \begin{bmatrix} l_q \\ t_q^{\partial} \end{bmatrix}$. This implies that q is dominated by q' and hence is not a Pareto path.

The other sub-case is $t^{\partial}_{q'} > t^{\partial}_{q}$. By definition, *Covered Element* gives $\epsilon^{k+1} \prec t^{\partial}_{q'}$. But $\epsilon^{k+1} < t^{\partial}_{q} \Rightarrow t^{\partial}_{q} = t^{\partial}_{q'}$, which is, again, a contradiction.

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

Note that the Algorithm 2 can be implemented in polynomial time complexity. Algorithm 2 uses arc exclusion to generate $P^{\text{Pruned}-\epsilon}_{ij}$, which can be implemented in $O(|V|^2)$ time complexity. It makes use of the shortest path procedure to compute $P^{\text{candidate}}$, which can be implemented in $O(|V|^3)$ time complexity. In the worst case, the **repeat-until** loop in Algorithm 2 iterates over all the covering relations of S_2. So the worst case time complexity of the algorithm is $O(|S_2|.|V|^3)$.

5.1.2. Biased routing strategy

This lexicographic efficiency class is represented by

$$\left(P_{ij}, \begin{bmatrix} l_p \\ t^{\partial}_p \end{bmatrix}, S_1 \times S_2^{\partial}, \leq_{lex}\right)$$

Based on the lexicographic ordering that we choose, we obtain length or trust biased routing strategies: the strategies that consider the length or the trust as superior metrics, respectively. It is well known that these lexicographic optimal paths can be solved at affordable complexity [22]. In this paper, we only present the semiring algebra for the length-lexicographic semiring. This problem is referred to as the shortest-widest path problem [12].
Length-lexicographic semiring: $(S = S_1 \times S_2^{\partial}, \oplus, \otimes)$. The semiring operations are defined as follows. For $(d1, t1^{\partial}), (d2, t2^{\partial}) \in S$ we define:

$$(d1, t1^{\partial}) \oplus (d2, t2^{\partial}) = \begin{cases} (d1, t1^{\partial}) & \text{if} \quad d1 < d2 \\ (d2, t2^{\partial}) & \text{if} \quad d2 < d1 \\ (d1, \min(t1^{\partial}, t2^{\partial})) & \text{if} \quad d1 = d2 \end{cases}$$

$$(d1, t1^{\partial}) \otimes (d2, t2^{\partial}) = (d1 + d2, \min(t1^{\partial}, t2^{\partial}))$$

It is shown that the SAPP problem for this semiring can be solved in a distributed manner [22]. The algorithm can be implemented using generalized Jacobi iterations in $O(|V|^3)$ time complexity.

5.1.3. Conservative routing strategy

Another efficiency for bi-objective optimization is the *Max-Ordering* (MO) method ([9]). However, this method is applicable to trusted routing only if the trustworthiness values and the path lengths are comparable. If they are, then we obtain a conservative routing strategy. This is represented by the tuple

$$\left(P_{ij}, \begin{bmatrix} l_p \\ t^{\partial}_p \end{bmatrix}, S_1 \times S_2^{\partial}, \leq_{MO}\right)$$

The above efficiency tries to select paths that 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 corresponding optimization problem is given by

$$\min_{p\in P_{ij}} \max\{l_p, t_p^{\partial}\} \tag{9}$$

Semiring decomposition: The MO problem involves the trust and length arc compositions. We present a decomposition method to separate the semirings. Eq. (9) can be written as

$$\begin{aligned} \min_{p\in P_{ij}} \quad & z \\ & l_p \leq z \\ & t_p^{\partial} \leq z \end{aligned}$$

Again, the decomposition yields an arc exclusion (Algorithm 1) and a shortest path procedure to obtain the MO paths. This is illustrated in Algorithm 3. The algorithm assigns an infinite cost to a non-existent path. In Algorithm 3, *Covering Element(x)* returns the covering element of $x \in S_2^{\partial}$.

Algorithm 3 Compute MO paths

$z \leftarrow \bot$
while True **do**
  $p^{\text{candidate}} \leftarrow arg \min_{p\in\mathcal{P}_{S,T}^{\text{Pruned}-\epsilon}} l_p$
  if $l_{p^{\text{candidate}}} \leq \epsilon$ **then**
    return $p^{\text{candidate}}$
  end if
  if $\epsilon = ?\top$ **then**
    return No path found
  end if
  $\epsilon \leftarrow$ *Covering Element*(ϵ)
end while

Proposition 5.3. *The path returned by Algorithm 3 is MO optimal in G.*

Proof. Since the sequence of ϵ's is monotone and S_2 is finite, the algorithm converges. When the algorithm terminates, $p^{\text{candidate}}$ has $l_{p^{\text{candidate}}} \leq \epsilon$ and $t^{\partial}_{p^{\text{candidate}}} \leq \epsilon$. And $\epsilon \in S_2^{\partial}$ is the smallest element for which this condition is satisfied. Thus $p^{\text{candidate}}$ upon termination is MO optimal. □

Similar to the Pareto optimal routing algorithm, the time complexity of this algorithm is $O(|S_2|.|V|^3)$.

The algorithms proposed in this section use the shortest path and arc exclusion routines repeatedly. This is a manifestation of the semiring decomposition. There are many other efficient polynomial-time distributed implementations for both of these routines [15]. Thus all these algorithms can be efficiently implemented in a self-organized MANET.

In all the algorithms discussed in this subsection, we have posed the selective arc composition, dual trust, as a constraint to obtain a reduced graph. Solving the SAPP for the other arc composition, path length, in the reduced graph yields the desired solution. Now, we return to the product monoid constructed in the start of this section, and we extend the above three algorithms for the general case. The fundamental idea, again, is to decouple the selective monoids $(S_l, \otimes_l)$, $2 \leq l \leq m$ from the arbitrary monoid $(S_1, \otimes_1)$ by graph reduction and then to solve the SAPP on the reduced graph for the arbitrary monoid.

5.2. Pareto efficiency

Consider the Pareto efficiency

$$(P_{ij}, \underline{w}, S, \leq_{com}).$$

The aggregate metric set for a pair of vertices $i, j \in V$ for Pareto efficiency is

$$x_{ij}^{f^{com}} = \oplus_{p\in P_{ij}}^{f^{com}} \underline{w}_p.$$

To apply the *Haimes-ϵ constraint* method, we need to extend it to handle partially ordered sets. The extended version of the *Haimes-ϵ constraint* method for the aggregate metric between vertices $i, j \in V$:

$$\begin{aligned} &\text{Min}_{p\in P_{ij}}\ \underline{w}_p(1) \\ &\text{subject to}\ \ \underline{w}_p(2..m) \leq \underline{\epsilon}, \end{aligned} \tag{10}$$

where $\underline{\epsilon} \in \times_{2\leq l\leq m} S_l$. Any solution to Eq. (10) is in the non-dominated aggregate metric set $x_{ij}^{f^{com}}$. The proof is similar to the standard *Haimes-ϵ constraint* method. Sweeping across different ϵ's we can obtain all the non-dominated solutions [9].

Applying the constraint method to the product monoid of interest decouples the constraints from the objective in Equation (10). The constraint $\underline{w}_p(2..m) \leq \epsilon$ implies that for a feasible path $p = (i = u_1, u_2, \ldots, u_n = j) \in P_{ij}$, for $2 \leq l \leq m$,

$$\begin{aligned} &\underline{c}_{u_1u_2}(l) \otimes_l \underline{c}_{u_2u_3}(l) \otimes_l \cdots \otimes_l \underline{c}_{u_{n-1}u_n}(l) \leq \underline{\epsilon}(l-1) \\ \Rightarrow\ &\min(\underline{c}_{u_1u_2}(l), \underline{c}_{u_2u_3}(l), \ldots, \underline{c}_{u_{n-1}u_n}(l)) \leq \underline{\epsilon}(l-1) \\ \Rightarrow\ &\underline{c}_{u_ku_{k+1}}(l) \leq \underline{\epsilon}(l-1)\ 1 \leq k < n. \end{aligned}$$

This implies that all the arcs along a feasible path must have $\underline{c}_{uv}(2..m) \leq \underline{\epsilon}$; all paths that have arcs $(u, v) \in A$ with $\underline{c}_{uv} > \epsilon$ must be discarded in searching for the non-dominant paths. The pruned set of paths can be obtained from a reduced graph, which is constructed by arc exclusion similar to Algorithm 1. For the general Pareto efficiency, this corresponds to replacing the arc metrics with ⓪ for arcs (u, v) that have $\underline{c}_{uv} > \underline{\epsilon}$. The absorbing property of $\oplus$ ensures that such paths are discarded while searching for non-dominant paths. It is convenient to define a modified arc metric

$$\underline{c}_{uv}^{\underline{\epsilon}} = \begin{cases} \underline{c}_{uv} & \text{if } \underline{c}_{uv}(2..m) \leq \underline{\epsilon} \\ ⓪ & \text{otherwise} \end{cases}$$

The problem with modified weights $\underline{c}_{uv}^{\epsilon}$ corresponds to the reduced graph. Let us denote the modified weights of the path by w_p^{ϵ}. Then the problem

$$\text{Min}_{p\in P_{ij}} \underline{w}_p^{\epsilon}(1)$$

yields a non-dominated solution. To obtain all the non-dominated solutions, specialized search methods that depend on the structure of the S should be employed. If the sets S_l, $2 \leq l \leq m$, are countable, then we can apply the same traversal algorithm of Section 5.1 to obtain all the Pareto efficient paths.

5.3. Lexicographic efficiency

Lexicographic efficiency is given by the tuple

$$(P_{ij}, \underline{w}, S, \leq com).$$

The aggregate metric problem for a pair of vertices $i, j \in V$ for the Lexicographic efficiency is

$$x_{ij}^{f^{lex}} = \oplus_{p\in P_{ij}}^{f^{lex}} \underline{w}_p.$$

The arc composition/product monoid of interest has a special structure that allows us to construct the following semiring. The product monoid with the lexicographic ordering, for $A, B \in 2^S$ yields a componentwise computation:

$$D = \{d \in A \cup B \ : \ d(1) \in \mathrm{Min}(e(1) : e \in A \cup B)\}$$

$$d', d'' \in D,$$

$$d' \oplus^{f^{lex}} d'' = \begin{cases} d' & \text{if } d'(1) < d''(1) \\ d'' & \text{if } d''(1) < d'(1) \\ d' & \text{if } d'(1) = d''(1) \\ & \quad \text{and } d'(2..,) \leq_{lex} d''(2..n) \\ d' \cup d'' & \text{if } d'(1) || d''(1) \end{cases}$$

This reduces the complexity of the path composition: for composing two path sets $A, B \in 2^S$, first, identify the set of paths D that is non-dominant in the first component $w_p(1)$, then for the comparable vectors apply the lexicographic ordering. The arc composition follows the standard *Minkowski product*.

5.4. Max-order optimality

Since the max-order optimality needs a total order on S, the most general version is that shown in the example of trusted routing. The max-order efficiency/optimality is given by the tuple

$$(P_{ij}, \underline{w}, S, \leq_{max}).$$

For the multi-metric problem, the max-order efficiency can be posed as an optimization problem:

$$\min_{p \in P_{ij}} \quad z$$

$$w_p(l) \leq z \ 1 \leq l \leq m.$$

This problem can be solved by the method proposed in Section 5.1.

6. Conclusion

We have developed a common framework to study multi-metric network problems specified using rules, where the metrics can be traditional network parameters such as delay or logical parameters such as trust. We have formulated path composition rules from multi-criteria optimization theory and shown that these rules can be viewed as instances of an idempotent SAPP called the efficiency SAPP. For each of the different order relations, used in multi-criteria optimization, we show that this efficiency SAPP yields different forms of efficiency, i.e., Pareto, lexicographic and max-order efficiency. We also identify an arc composition rule that is solvable in each of these efficiencies with affordable computational complexity. As an application of this arc composition rule, we show that it can be applied to trusted routing in MANETs.

Acknowledgements

This material is based upon work supported by the MURI Award Agreement W911-NF-0710287 from the Army Research Office and by DARPA under award number 013641-001 for the Multi-Scale Systems Center (MuSyC) through the FRCP of SRC and DARPA.

References

[1] K. Aberer, 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.

[2] S. Bansal, M. Baker, Observation-based Cooperation Enforcement in Ad hoc Networks, Technical Report, Stanford University, 2003.

[3] J.S. Baras, G. Theodorakopoulos, Path problems in networks, in: Synthesis Lectures on Communication Networks, Morgan and Claypool, 2010
[4] S. Buchegger, J.-Y. Le Boudec, A robust reputation system for p2p and mobile ad-hoc networks, in: Proceedings 2nd Workshop on the Economics of P2P Systems, 2004.
[5] V. Chankong, Y.Y. Haimes, Multiobjective Decision Making: Theory and Methodology, Elsevier Science Publishing Co., Inc., 1983.
[6] R. Chen, W. Yeager, Poblano: A Distributed Trust Model for Peer-to-peer Networks, Technical Report, Sun Microsystems, 2001.
[7] F. Cornelli, E. Damiani, Di S. De Capitani, S. Paraboschi, P. Samarati, Choosing reputable servants in a p2p network, in: Proceedings of the 11th World Wide Web Conference, 2002, pp. 376–386
[8] B.A. Davey, H.A. Priestley, Introduction to Lattices and Order, Cambridge University Press, 1990.
[9] M. Ehrgott, Multicriteria Optimization, Springer, 2005.
[10] J.S. Golan, Semirings and their Applications, Kluwer Academic Publishers., 1999.
[11] M. Gondran, M. Minoux, Graphs Dioids and Semirings – New Models and Algorithms, Springer, 2008.
[12] T.G. Griffin, The stratified shortest-paths problem, in: Proceedings of the 2nd International Conference on Communication Systems and Networks, 2010, pp. 268–277.
[13] Y.Y. Haimes, L.S. Lasdon, D.A. Wismer, On a bicriterion formulation of the problems of integrated system identification and system optimization, IEEE Trans. Systems Man Cybernet. 1 (1971) 296–297.
[14] J. Hu, M. Burmester, Lars: a locally aware reputation system for mobile ad hoc networks, in: 44th ACM Annual Southeast regional Conference, 2006, pp. 119–123.
[15] J. Kleinberg, E. Tardos, Algorithm Design, Addison Wesley, 2005.
[16] V.N. Kolokoltsov, Idempotent structures in optimization, J. Math. Sci. 104 (1) (2001) 847–880.
[17] V.N. Kolokoltsov, V.P. Maslov, Idempotent Analysis and its Applications, Kluwer Academic Publishers., 1997.
[18] G. Nicolescu, P.J. Mosterman (Eds.), Model-based Design of Embedded Systems, CRC Press, 2010.
[19] A.A. Rahman, S. Hailes, A distributed trust model, in: Proceedings of the 1997 Workshop on New Security Paradigms, 1998, pp. 8–60.
[20] G. Rote, Path problems in graphs, Comput. Suppl. 7 (1990) 155–189.
[21] S.N. Samborskii, A.A. Tarashchan, The fourier transform and semirings of pareto sets, in: V.P. Maslov, S.N. Samborskii (Eds.), Idempotent Analysis, Advances in Soviet Mathematics, AMS, 1992, pp. 139–150.
[22] K.K. Somasundaram, J.S. Baras, Path Optimization Techniques for Trusted Routing in Mobile Ad-hoc Networks: An Interplay between Ordered Semirings, Technical Report, Institute of Systems Research, University of Maryland, College Park, 2008.
[23] K.K. Somasundaram, J.S. Baras, Path Optimization Techniques for Trusted Routing in Tactical Mobile Ad-hoc Networks, Technical Report, Institute of Systems Research, University of Maryland, College Park, 2008.
[24] G. Theodorakopoulos, J.S. Baras, On trust models and trust evaluation metrics for ad hoc networks, IEEE J. Sel. Areas Commun. 24 (2) (2006) 318–328.
[25] L. Xiong, L. Liu, A reputation-based trust model for peer-to-peer ecommerce communities, in: Proceedings of the 4th ACM Conference on Electronic Commerce, 2003, pp. 228–229.
[26] P.R. Zimmermann, The Official PGP User's Guide, MIT Press, 1995.
[27] R. Zurawski (Ed.), Embedded Systems Handbook: Network Embedded Systems, CRC Press, 2009.