This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

A Formal Study of Trust-Based Routing in Wireless Ad Hoc Networks

Chi Zhang*, Xiaoyan Zhu†, Yang Song* and Yuguang Fang*†
*Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611, USA
†National Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China

***Abstract*—Recently, trust-based routing has received much attention as an effective way to improve security of wireless ad hoc networks (WANETs). Although various trust metrics have been designed and incorporated into the routing metrics, as far as we know, none of the existing works have used mathematical tools such as routing algebra to analyze the compatibility of trust related routing metrics and routing protocols in WANETs. In this paper, we first identify unique features of trust metrics compared with QoS-based routing metrics. Then, we provide a systematic analysis of the relationship between trust metrics and trust-based routing protocols by identifying the basic algebraic properties that a trust metric must have in order to work correctly and optimally with different generalized distance-vector or link-state routing protocols in WANETs. Moreover, we extend our framework to model the interactions between different trust-based routing protocols. Finally, our results are applied to check the compatibility of the trust metrics proposed in previous literature and the popular routing protocols used in WANETs.**

I. Introduction

A *wireless ad hoc network* (WANET) is a collection of wireless mobile nodes dynamically forming a temporary network without requiring any centralized authority or fixed network infrastructure [1]–[3]. Neighboring nodes can directly communicate through wireless links, while faraway nodes are connected by distributed routing protocols. Due to their open, distributed and dynamic nature, WANETs are highly vulnerable to various (external or internal) malicious attacks [2], [3]. To improve security of WANETs, one natural idea is to include trust relationships between individual nodes, i.e., who trusts who and how, into route / path selection decisions. To facilitate the implementation of this idea, various *trust metrics*, which quantify trust relationships according to different applications' security requirements, have been designed and integrated into routing metrics[1] in the literature. For example, PGP-style authentication schemes with certification chains [4], [5] use a binary trust valuation (e.g., 1-or-0, all-or-none). Reputation-based schemes [6], [7] employ real numbers to measure the trustworthiness. In some evidence-based schemes [8], [9], a two-dimensional vector in $[0, 1]^2$ describes the trust opinion. In [10], trust measurement is even combined with other QoS requirements to act as the routing metric (cf. Section II-D for detailed discussions).

While these application-specified trust metrics capture different characteristics of their target scenarios or trust relationships, there is a lack of understanding on the impact of trust metrics on the operations of routing protocols. One important lesson we have learned from Internet routing protocol design is that in general we cannot arbitrarily change one routing metric to another without considering the routing protocols used in the network. If routing metrics are unscrupulously combined with an incompatible routing protocol, the routing protocol may fail to find an optimal path or lead to routing loops [11], [12]. This principle is still applicable here, since the trust metric is just a special kind of routing metrics, and routing protocols in WANETs share many common features with their Internet counterparts [1], [13]. In fact, our case study shows that some trust metrics mentioned above lead to routing anomalies when they are combined with a Dijkstra-based routing algorithm (cf. Section IV for detailed discussions).

In the networking research community, a theoretical framework called *routing algebra* has been developed for the study of the compatibility of routing metrics and routing protocols in the context of QoS routing [11] and BGP protocols [12] used in the Internet. It has also been extended and applied to multi-hop wireless networks recently [13], [14]. *So why do not we just use the existing routing algebras mentioned above to study trust metrics* (as a part or total routing metrics)? The key point here is that trust metrics are significantly different from normal routing metrics such as the number of hops, data rates or other QoS requirements. In what follows, we identify four unique features of trust metrics, which make previous results unapplicable to trust-based routing.

First of all, *the topological structures related to trust metrics are more complicated*. Trust relationships among individual nodes form a new topological structure called trust graph, which may have totally different structures compared with the physical link graph. Trust-based routing is restricted by the physical conditions as well as trust conditions, and therefore requires a new routing algebra built upon both graphs. Secondly, *trust metrics have different algebraic properties compared with normal routing metrics.* For example, in Section III-C, we will show that trust metrics in general are non-distributive, while most of previous routing algebras assume that distributivity holds [11]–[13]. Thirdly, for traditional routing metrics, the metric value of one physical link is independent of that of other links. However, trust can be passed (propagated) between different users, which means *the trust-based routing metrics of different physical links are dependent*. Obviously, this dependency will complicate the analysis of trust-based routing. Lastly, different groups of people may have different rules to establish and handle trust, and therefore, *trust metrics are group dependent and non-uniform*. When an end-to-end communication runs across multiple groups, more effort needs to be made to model the inter-operation between different trust-based routing protocols.

To sum up, the diversity and complexity of trust metrics require a systematic analysis of their properties and the corresponding relationships with routing protocols. By developing

This work was partially supported by the U.S. National Science Foundation under grants CNS-0916391, CNS-0716450, CNS-0721744 and CNS-0626881, and China 111 Project under grant B08038. The work of X. Zhu was also partially supported by the National Natural Science Foundation of China under Grant 60772136 and the 863 Project of China under Grant 2007AA01Z435.

X. Zhu is currently a visiting research scholar with Department of Electrical and Computer Engineering, University of Florida. Y. Fang is also a Changjiang Scholar Chair Professor with National Key Laboratory of Integrated Services Networks, Xidian University, China.

[1]In what follows, when the trust metric is utilized as a (part of) routing metric, we call the later as the *trust related routing metric*, or just *trust metric* for short, and the corresponding routing protocol as *trust-based routing*.

978-1-4244-5837-0/10/$26.00 ©2010 IEEE

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

formal models to describe different trust environment, our paper identifies the basic algebraic properties that a trust metric must have in order to work with different generalized distance-vector or link-state routing protocols in WANETs.

II. Abstract Framework and Motivating Examples

In this section, we first develop an abstract framework to facilitate our study on trust-based routing protocols. Then we utilize some simplified examples to provide our motivation for developing the formal approach adopted in this paper.

A. System Model for Trust Management

In general, *trust management* in any communication systems can be modeled as a procedure with three sequential phases:

Phase 1: direct trust establishment. Direct trust relationships can be obtained from the evidence created by the previous interactions or inherited from the pre-established social relationships in the physical world. In the former case, local monitoring schemes like Watchdog and Pathrater [15] and physical contact scheme [16] have been proposed to collect the first-hand trust evidence. In the latter case, participating node only needs to verify the other side's identity [5] based on cryptographic primitives. Trust evaluation module then transforms the trust evidence or inherent trust relationships into direct trust metrics (i.e., quantitative descriptions of trust).

Phase 2: indirect trust inference. When the trust relationships are (at least partly) transitive, more trust relationships (or *indirect trust*) can be derived from the direct trust. First of all, direct trust information need be propagated throughout the network. Any information gossip protocol or broadcast protocol can fulfill this task, and no specific path selection scheme is needed here. We also assume that appropriate cryptographic primitives are available in WANETs in order to provide a secure propagation of direct trust information. Then, based on these second-hand trust evidence, each node can establish new indirect trust relationships with its physical neighbors of which it knows nothing. Trust-based routing is differentiated from traditional routing by introducing trust inference as one of important preprocessing for path selection and packet forwarding, and therefore should be explicitly considered in our modeling. Note that when direct trust relationships are all non-transitive, no indirect trust can be derived from phase 2.

We distinguish two kinds of trust in this paper: *transitive* and *non-transitive trust*. For transitive trust, if node v_i has trust $t(i,j)$ in node v_j, and v_j has trust $t(j,k)$ in node v_k, then v_i should have some trust $t(i,k)$ in v_k that is a function of $t(i,j)$ and $t(j,k)$. For non-transitive trust, however, we cannot obtain any conclusion on $t(i,k)$, given $t(i,j)$ and $t(j,k)$. We note that transitive trust (and consequently, indirect trust) is important for any trust-based routing to be practical in large-scale dynamic WANETs. Because of the large number of nodes and node mobility, it is impossible for one node to have direct trust with any of its physical neighbors. When the physical link between two nodes is needed to perform multi-hop routing, the trust on this link must be derived beforehand.

Phase 3: trust-based operations. Direct and indirect trust established in previous two phases will be utilized to support all operations in this phase. For trust-based routing, trust-related routing metrics will be formed (e.g., combined with other QoS metrics) and used as the criteria for selecting most trustworthy paths between any source-destination (S-D) pair.

Phase 1 only concerns with the forming and evaluation of direct trust with neighboring nodes and has no direct relations with routing problem, which is orthogonal and complementary to the research described here and therefore excluded from the rest discussions of this paper. Based on above discussions, we can identify two elementary operations, namely, trust inference and trustworthy path selection for any trust-based routing protocols, which will be investigated here.

B. Graph Models for WANETs

We utilize graph models to describe physical resources and trust relationships in a WANET. Therefore, we first review some basic concepts applicable to any graph model. For a *labeled direct graph* $G = (V, E, \omega)$, V is the vertex set, $E \subseteq V \times V$ is the edge / link set, and ω is a function which assigns each link $e \in E$ a label $\omega(e)$. Labels here are the abstraction of routing metrics or trust metrics on links. We also extend this concept to a path, i.e., the label $\omega(p)$ of a path p, which is the metric measuring the whole path. For edge $(i,j) \in E$, we say that node v_j is an *out-neighbor* of node v_i, and that node v_i is an *in-neighbor* of node v_j. The set of out-neighbors of node v_i is denoted as N_i. A *path* p from v_1 to v_n is denoted by $p(v_1, v_n) = \langle v_1, v_2, \cdots, v_n \rangle$ and $p_{1,n}$ for short. If the last node of path p coincides with the first node of path q, the $p \circ q$ denotes the path formed by the concatenation of p and q. A path is *simple* or *loop-free* if all nodes from v_1 to v_n are distinct. If $v_1 = v_n$, we say $p_{1,n}$ forms a *loop*.

The physical resources of a WANET are modeled by *physical graph* $G_H(V,E_H,h)$ where E_H is the set of directed edges representing wireless links[2]. The direct trust relationships are modeled as *trust graph* $G_T(V,E_T,t)$ where E_T is the set of directed edges representing direct trust relationships. When trust is transitive, we can derive *augmented trust graph* $G_T^*(V,E,it)$ based on $G_T(V,E_T,t)$ and indirect trust inference scheme, where $E = H \times H$. For a link $(i,j) \in E_H$, the routing metric of that link is measured by a function $r(i,j)$, i.e.,

$$r(i,j) \triangleq \begin{cases} r\left(p(i,j), t(i,j)\right) & \text{for non-transitive trust} \\ r\left(p(i,j), it(i,j)\right) & \text{for transitive trust} \end{cases},$$

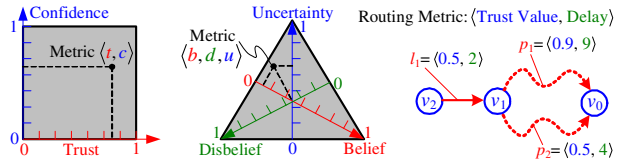
which converts the combination of physical properties and trust relationship into a trust related routing metrics. Graph $G_R(V,E_R,r)$ is called *routing graph*, because trustworthy path selection and packet forwarding are actually performed on it. When trust metrics are directly used as routing metrics, $r(i,j) = t(i,j)$. Note that, even in this case, trust/routing metrics are still constrained by physical graph, because $E_R = E_H$. Due to the node mobility and limited communication range of wireless communication techniques, $G_T(V,E_T,t)$ may have totally different topological structure from that of $G_H(V,E_H,h)$. This property distinguishes our study from previous work on trust inference or trust-based routing in P2P networks or on-line social networks [17], where the trust graph and the physical graph are assumed to have the same topology.

C. Formalizing Routing Protocols

Given the routing graph, for any hop-by-hop routing protocol, its main task is to find a path between each S-D pair with the desirable properties (defined by routing metrics). Because for each destination, i.e., v_0, every source will have in its routing table the next hop to reach that destination, a spanning tree rooted at each destination is defined implicitly by the set of routing tables residing in a network. We call this spanning tree as *in-tree* with the root node as the given destination

[2]This wireless link can be generalized as any physical link which can flow packets between two nodes. For example, in a WANET with partial infrastructure, this link can also be a wired link. In a delay-tolerant network (DTN), this link can be two wireless links combined with one node movement.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.



(a) A pair as trust metric (b) A triple as trust metric (c) Combined metric

Fig. 1. **Diversity of trust metrics.**

v_0. Therefore, any routing protocol can be abstracted as the collection of rules and procedures to generate an in-tree for a given destination.

To facilitate the comparison between labels (i.e., routing metrics) of different paths, we define a *total pre-order*[3] $\preccurlyeq$ over R, the label set of G_R. For two paths p and q in $G_R(V,E_R,r)$, if $r(p) \preccurlyeq r(q)$, we say that p is *weakly preferred* to q (e.g., path p is at least as trustworthy as path q). If $r(p) \preccurlyeq r(q)$ and $r(q) \preccurlyeq r(p)$, then we write $r(p) \sim r(q)$ and say that p and q are *equally preferred*. Relation $r(p) \prec r(q)$ means that $r(p) \preccurlyeq r(q)$ and $r(p) \not\sim r(q)$, i.e., *strictly preferred*. Functions max and min are defined with respect to $\preccurlyeq$.

The existing hop-by-hop routing protocols in WANETs can be divided into two categories according to their different path selection approaches: namely, *link-state routing* and *distance-vector routing*: (1) In the *link-state* approach to routing, each node broadcasts updates of its local topology information (link state) to the rest of the network. These broadcasts can be periodic or event-driven. By putting the updates together, each node is able to reconstruct the routing graph $G_R(V,E_R,r)$ for the entire network. Given $G_R(V,E_R,r)$, a node can then construct its routing tables appropriately by running Dijkstra's shortest path algorithm (when taking the distance as the routing metric). For the general routing metrics, a generalized Dijkstra's algorithm is used. Given the destination v_0, each node v_i will calculate the *most preferred path* $p^*_{i,0}$ on $G_R(V,E_R,r)$, according to $r(p^*_{i,0}) = \min\{r(p_{i,0}) \mid \forall p_{i,0} \in \mathcal{P}_{i,0}\}$, where $\mathcal{P}_{i,0}$ is the set of all paths from v_i to v_0. When v_j is the next-hop node on path $p^*_{i,0}$, we have $x_i = r(i,j) \otimes x_j$ [4] where $v_j \in N_i$. Exemplary routing protocols for WANETs in the literature which fall into this category include LQSR, HSR, OLSR and HSLS [1]. (2) In the *distance-vector* approach to routing, neighboring nodes exchange (advertise) vectors of distances with each other. Each entry in a distance-vector corresponds to a particular destination and contains the current distance estimate of the shortest path from the source to the corresponding destination. For the general routing metrics, it means that each node v_i only knows its out-neighbors, its out-going links, and its out-neighbors' node labels. Node v_i will calculate its own node label x_i (which has one-to-one mapping with the entry in routing table for v_0 and the selected path $p_{i,0}$) using a generalized Bellman-Ford algorithm: $x_i = \min\{r(i,j) \otimes x_j \mid \forall v_j \in N_i\}$. Exemplary routing protocols for WANETs in the literature which fall into this category include AODV and DSDV [1].

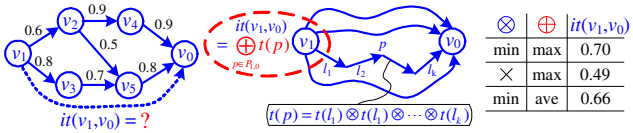
Based on above discussions, we can naturally introduce our definitions on the *correctness* and *optimality* of any routing protocol $\mathcal{R}$ as follows:

***Definition** 1:* **[$\mathcal{R}$-Correctness]** A (trust-based) routing protocol $\mathcal{R}$ is *correct* if given any $G_R(V,E_R,r)$ and destination node v_0, the next-hop nodes calculated by $\mathcal{R}$ form an in-tree.

***Definition** 2:* **[$\mathcal{R}$-Optimality]** A (trust-based) routing protocol $\mathcal{R}$ is *optimal* if given any $G_R(V,E_R,r)$ and destination node v_0, (1) the next-hop calculated by $\mathcal{R}$ form an in-tree and (2) for every node v_i $(i \neq 0)$, packets will be forwarded along the most preferred path $p^*_{i,0}$ among all existing physical paths from v_i to v_0.

[3]Recall that a pre-order is a reflexive and transitive relation.

[4]Operator $\otimes$ represents combination operation of serial labels along a path. Please refer to Section III for a detailed discussion.



⊗	⊕	$it(v_1,v_0)$
min	max	0.70
×	max	0.49
min	ave	0.66

(a) Trust inference problem (b) Algebraic path problem (c) Examples

Fig. 2. **Algebraic path formulation for indirect trust inference problems.**

D. Motivating Examples

Example 1: diversity of trust metrics. Consider a reputation system based on direct interactions. A node's experience with another node is modeled as a binary event: positive or negative. Evidence $\langle r, s\rangle$ is conceptualized in terms of the numbers of positive (r) and negative (s) experiences. Based on this simple evidence space, various trust metrics are proposed in the literature, according to different design rationale:

- a trust value in the real interval $[0,1]$; [6]
- a pair $\langle t, c\rangle$ in $[0,1]^2$, where t and c represent trust and confidence value (see Fig. 1 (a)); [8]
- a triple $\langle b, d, u\rangle$ in $[0,1]^3$, where b, d and u represent belief, disbelief and uncertainty value, respectively, and $b+d+u=1$ (see Fig. 1 (b)). [9]

Even for the simplest trust value, when it is combined with other QoS requirements [10], routing anomalies will emerge. Consider the routing graph given in Fig. 1 (c). Let routing metric be of the form $\langle t, d\rangle$, where t is trust value and d is delay. The label for a path p will be $\langle t_p, d_p\rangle$, where t_p is the minimal trust value of links along the path and d_p is the delay addition along the path. Order $\preccurlyeq$ is defined as a lexicographic order: $\langle t_1, d_1\rangle \preccurlyeq \langle t_2, d_2\rangle \Leftrightarrow t_1 > t_2$ or $(t_1 = t_2$ and $d_1 \leq d_2)$, where trustworthy paths are preferred, with small delays breaking ties. The in-tree for the destination v_0 found by any routing protocol consists of link l_1 and path p_1. For node v_1 path p_1 is optimal; however, for node v_2 path $l_1 \circ p_1$ is not better than $l_1 \circ p_2$, because $r(l_1 \circ p_1) = \langle 0.5, 11\rangle$ and $r(l_1 \circ p_2) = \langle 0.5, 6\rangle$. Obviously, $\langle 0.5, 6\rangle \preccurlyeq \langle 0.5, 11\rangle$. This simple example demonstrates that for the routing metric of the form $\langle t, d\rangle$ defined above, no routing protocol will be optimal.

Example 2: diversity of operations on trust metrics. Consider an indirect trust inference problem like the one given in Fig. 2 (a). Here solid lines represent direct trust. The number on each link represents the trust value. We want to infer the indirect trust value $it(v_1, v_0)$ from v_1 to v_0 based on direct trust values. There also exist various ways in the literature to fulfil this task (refer to [8] and [17] and the references therein):

- We could choose the strongest path, determined by the path with the highest minimum value, and take the lowest value on that path as $it(v_1, v_0)$. Based on this inferring scheme, the strongest path is $\langle v_1, v_3, v_5, v_0\rangle$ with $it(v_1, v_0) = 0.7$.
- We could choose the strongest path, determined by the path with the highest product of all values on the path, and take the product of all values on that path as $it(v_1, v_0)$. Based on this inferring scheme, the strongest path is $\langle v_1, v_2, v_4, v_0\rangle$ with $it(v_1, v_0) = 0.49$.
- Trust value $it(v_1, v_0)$ can be calculated as the weighted average of the minima of the trust values along the disjoint paths. The weights in the average are given by v_1's trust in its direct out-neighbors. According to this inferring scheme, $it(v_1, v_0) = 0.66$.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

Every indirect trust inference scheme mentioned above has its own pros and cons. Here, we are not interested in judging their usefulness according to different application scenarios, instead, we are focusing on developing an abstract framework so that we can reason about their behavior as a whole. For trust inference problem, we know that we can apply a mathematical tool called *path algebra* [18]–[20]. We can define an operator $\otimes$ to concatenate trust metrics along a path, then we introduce another operator $\oplus$ to aggregate trust metrics across paths (see Fig. 2 (b) for an illustration). When $\oplus$ and $\otimes$ satisfy certain properties, using path algebra, the problem of calculating $it(v_1, v_k)$ can be formulated uniformly as the one given in Fig. 2 (b). From Fig. 2 (c), we observe that all trust inference algorithm mentioned above can be included in this formulation with different interpretations of $\otimes$ and $\oplus$.

These two examples suggest that, instead of examining every possible trust metrics and operations one by one, we can study their behaviors as a whole by developing an algebraic formalism that abstracts trust relationships and also link resources as labels, and models the routing operations as certain operators on the labels. What related to the correctness and optimality of routing protocols are not the contents (the meaning of these trust metrics), but their algebraic properties. Therefore, we need describe, classify and analyze different trust metrics and operators based on their algebraic structures.

III. Path Algebra for Indirect Trust Inference

In this section, we develop a non-classical path algebra based on bi-monoid to study indirect trust inference problems.

A. Algebraic Foundations

The general frameworks used in this and next sections are based on the algebraic structure of semigroups and monoids. Thus, we first briefly review some relevant results.[5]

A *semigroup* $(S, \oplus)$ is a non-empty set S with a binary operator $\oplus$ such that (for all $a, b, c \in S$)

- $a \oplus b \in S$ ($\oplus$-Closure),
- $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ ($\oplus$-Associativity).

Moreover, a semigroup $(S, \oplus)$ is called (for all $a, b \in S$)

- *commutative* when $a \oplus b = b \oplus a$ ($\oplus$-Commutativity),
- *idempotent* when $a \oplus a = a$ ($\oplus$-Idempotency),
- *selective* when $a \oplus b = a$ or b ($\oplus$-Selectivity).

Note that a selective semigroup must be idempotent, but the converse is not true.

A semigroup $(S, \oplus)$ may have some special elements:

- $\varepsilon \in S$ is an *identity* if $\forall a \in S : \varepsilon \oplus a = a \oplus \varepsilon = a$,
- $\sigma \in S$ is an *annihilator* if $\forall a \in S : \sigma \oplus a = a \oplus \sigma = \sigma$,
- $a^{-1} \in S$ is an *inverse* of $a \in S$, if $a \oplus a^{-1} = a^{-1} \oplus a = \varepsilon$.

Note that ε, σ and a^{-1} defined above are unique if they exist. A semigroup is a *monoid* if it has an identity. A monoid is a *group* if $\forall a \in S : a^{-1}$ exists.

For a *commutative monoid* $(S, \oplus)$, it is always possible to introduce a pre-order relation over S, denoted $\preccurlyeq_\oplus$, as:

$$\forall a, b \in S : a \preccurlyeq_\oplus b \Leftrightarrow \exists c \in S : a = b \oplus c.$$

We call this relation as *canonical pre-order*, since the identity and associativity of $\oplus$ ensure that $\preccurlyeq_\oplus$ is indeed a pre-order. Note that $\oplus$-commutativity ensures that the following definition of $\preccurlyeq_\oplus$ are equivalent:

$$\exists c \in S : a = b \oplus c \Leftrightarrow \exists c \in S : a = c \oplus b.$$

The canonical pre-order $\preccurlyeq_\oplus$ has the following properties:

- If ε ($\oplus$-identity) exists, then $\forall a \in S : a \preccurlyeq_\oplus \varepsilon$.
- If σ ($\oplus$-annihilator) exists, then $\forall a \in S : \sigma \preccurlyeq_\oplus a$.

[5]See [18]–[21] for a more complete survey of the issues exposed here.

B. Formalizing Indirect Trust Inference Problem

After trust propagation subphase, every node will know the trust graph. If the trust is transitive, the functionality of trust inference is to calculate the indirect trust based on the trust graph. Here, we first formalize this procedure as follows.

Given the trust graph $G_T(V,E_T,t)$, where $t : E_T \mapsto T$ is a function which assigns each edge $e \in E_T$ a label $t(e) \in T$ (i.e., the direct trust metric on e), we need to compute the indirect trust metric $it(v_i, v_j)$ for every $(v_i, v_j) \in V \times V$. We first introduce two operations over the labels:

- *Concatenation* of serial labels with operator $\otimes$,
- *Aggregation* of parallel labels with operator $\oplus$.

Mathematically, $\otimes, \oplus : T \times T \mapsto T$ are two functions which combine two labels into a new one. Therefore, the label of a nontrivial path $p_{1,k} = \langle v_1, v_2, \cdots, v_k \rangle$ (i.e., the trust metric of path $p_{1,k}$) of G_T, denoted $t(p_{1,k})$, is given by

$$t(p_{1,k}) \triangleq (\cdots((t_{1,2} \otimes t_{2,3}) \otimes t_{3,4}) \cdots) \otimes t_{k-1,k},$$ [6]

and $t(p_i) \triangleq \bar{1}$ for trivial path $p_i = \langle v_i \rangle$.

A *solution* to an indirect trust inference problem is a function $it : V \times V \mapsto T$ such that $it(v_i, v_i) \triangleq \bar{1}$ and for all $i \neq j$, $it(v_i, v_j) \triangleq \bigoplus_{p \in \mathcal{P}(i,j)} t(p)$, where $\mathcal{P}(i, j)$ is the set of all paths from v_i to v_j. Given all $it(v_i, v_j)$, we can obtain augmented trust graph $G_T^*(V,E,it)$.

In this paper, we solve this problem within the following algebraic structure, called bi-monoid:

Definition 3: **[Bi-Monoid]** Given a trust graph G_T, we define the *non-classic path algebra* over G_T as an algebraic structure $(T, \oplus, \otimes, \bar{0}, \bar{1})$, where

- $(T, \oplus, \bar{0})$ is a commutative monoid with $\bar{0}$ as its identity,
- $(T, \otimes, \bar{1})$ is a monoid with $\bar{1}$ as its identity,
- $\oplus$-identity $\bar{0}$ is also an annihilator for $\otimes$.

We call this algebraic structure $(T, \oplus, \otimes)$ as *bi-monoid*.

From Section III-A, we know that there exists a canonical pre-order $\preccurlyeq_\oplus$ over T. We indicate it as $\preccurlyeq$ for short.

In previous work like [8], trust inference problems are solved within the algebraic structure called semiring:

Definition 4: **[Semiring]** A bi-monoid $(T, \oplus, \otimes, \bar{0}, \bar{1})$ is a *semiring* if $\otimes$ distributes over $\oplus$, i.e., for all $a, b, c \in T$:

- $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$ (Left Distributivity),
- $c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b)$ (Right Distributivity).

C. Verifying Bi-Monoid Properties

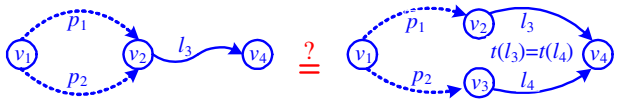
Here we give the physical meanings of the properties we impose on the algebraic structure of trust metrics in Def. 3 and explain why these properties should hold for trust metrics in practice. Remember that we need to keep the property set as minimal as possible in order to leave more room for trust metric design.

The associativity for both $\otimes$ and $\oplus$ operators allows the incremental calculation of trust metrics: If one more label needs to be aggregated into the current "total," then it can be done in one step, without having to recall all labels that were aggregated for the current total. The same goes for concatenation. Commutativity for aggregation $\oplus$ makes irrelevant the order in which labels are taken into account (i.e., which one is first, which one is second, etc.).

The $\bar{0}$ element (identity for $\oplus$, annihilator for $\otimes$) corresponds to nonexistent trust relations between nodes. The rationale is that if $\bar{0}$ is encountered along a path, then the whole path "through" this relation should have label equal to $\bar{0}$. Also, such paths should be ignored in $\oplus$-aggregation.

[6]When $\otimes$ is commutative, it equals to $t(p_{1,k}) \triangleq t_{1,2} \otimes t_{2,3} \otimes \cdots \otimes t_{k-1,k}$.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.



(a): $(t(p_1)\oplus t(p_2))\otimes t(l_3)$ (b): $(t(p_1)\otimes t(l_3))\oplus(t(p_2)\otimes t(l_3))$

Fig. 3. **Distributivity of trust metrics.**

The $\bar{1}$ element (identity for $\otimes$) corresponds to the most trustworthy relations between nodes. This can also be seen as the trust relation of a node with itself (i.e., trivial path in G_T). If a path is extended with a link of label $\bar{1}$, the path label should remain the same.

The key difference between our work and previous work is that our model does *not* impose distributivity on trust metrics. Here we illustrate our reason with an example. Consider two trust graphs given in Fig. 3 (a) and (b). In both graphs, $t(p_1)$ and $t(p_2)$ are path labels for two disjoint paths p_1 and p_2, respectively; $t(l_3)$ and $t(l_4)$ are link labels for link l_3 and l_4, respectively, with $t(l_3) = t(l_4)$. Now, we are trying to infer the indirect trust $t(v_1, v_4)$. Using path algebra, $t(v_1, v_4)$ in Fig. 3 (a) and (b) can be expressed as $(t(p_1) \oplus t(p_2)) \otimes t(l_3)$ and $(t(p_1) \otimes t(l_3)) \oplus (t(p_2) \otimes t(l_3))$, respectively. The question is whether these two expressions are equal for trust metrics?

We answer this question by examining the physical meanings of two trust graphs, respectively. For Fig. 3 (a), v_4 has only one in-neighbor, i.e. v_2, which means that only v_2 has direct interactions (direct trust) with v_4 before. Therefore, v_2 will act as witness to provide report about v_4's trustworthiness based on its own experience, which is measured by $t(l_3)$. Node v_1 will obtain two reports from two independent paths p_1 and p_2, with both reports claiming that the trustworthiness of v_4 is $t(l_3)$. The trustworthiness for the first report itself (from path p_1) is $t(p_1)$, while for the second report (from path p_2) is $t(p_2)$. For Fig. 3 (b), v_1 also obtain two reports stating the trustworthiness of v_4 is $t(l_3)$, and the trustworthiness for reports themselves are $t(p_1)$ and $t(p_2)$, respectively. It seems that from the view point of v_1, there is no difference between two situations. Unfortunately, this is not true. One key observation is that, in Fig. 3 (a), these two reports are issued by the same nodes v_2, while in Fig. 3 (b) these two reports are issued by two different nodes v_2 and v_3 separately. Therefore, although node v_1 collects the same second-hand evidence (two reports) on v_4 in two situations, in Fig. 3 (a) all theses evidence come from a single source v_2 while in Fig. 3 (b) they come from independent sources v_2 and v_3. Therefore, v_4 is more trustworthy for v_1 in Fig. 3 (b). This example shows that distributivity may not hold for trust metrics.

Next, we introduce a new property of trust metrics, which is not included in our bi-monoid model (i.e., Def. 3), but we believe it should hold in practice, since any path with label $\bar{1}$ is most preferred.

***Definition** 5:* **[Absorptivity]** A trust graph $G_T(V,E_T,t)$ is said to be *absorptive* if for every simple directed cycle $c = \langle v_1, v_2, \cdots, v_k, v_1\rangle$ in G_T, we have $\bar{1} \preccurlyeq t(c)$.

Absorptive graph is a generalization of the absence of a negative cycle in a graph with real numbers as edge weights. It plays an important role to make sure the solution of trust inference problem exists.

D. Solving Path Algebraic Problems

1) Solving the Problem with Semirings: We first recall how to solve a trust inference problem within the framework of semiring. The operations $\oplus$ and $\otimes$ can be extended in the usual way to matrices built from the elements of the set T. Let $\mathcal{M}_n(T)$ denote the set of all $n\times n$ matrices over T, and for $\mathbf{A}\in\mathcal{M}_n(T)$ let $\mathbf{A}_{ij}$ denote the (i,j)-entry of $\mathbf{A}$. For all $\mathbf{A},\mathbf{B}\in\mathcal{M}_n(T)$, we define $\mathbf{A}\oplus\mathbf{B}$ and $\mathbf{A}\otimes\mathbf{B}$ by $(\mathbf{A}\oplus\mathbf{B})_{ij} \triangleq \mathbf{A}_{ij}\oplus\mathbf{A}_{ij}$ and $(\mathbf{A}\otimes\mathbf{B})_{ij} \triangleq \bigoplus_{k=1}^{n}(\mathbf{A}_{ik}\otimes\mathbf{B}_{kj})$.

The $\oplus$-identity matrix $\bar{\mathbf{0}}$ and $\otimes$-identity matrix $\bar{\mathbf{1}}$ are given by:

$$\bar{\mathbf{0}}_{ij} \triangleq \bar{0} \quad \text{and} \quad \bar{\mathbf{1}}_{ij} \triangleq \begin{cases} \bar{1} & \text{if } i=j, \\ \bar{0} & \text{otherwise.} \end{cases}$$

Then $(\mathcal{M}_n(T), \oplus, \otimes)$ form another semiring.

The *adjacency matrix* $\mathbf{A}$ of the trust graph $G_T(V,E_T,t)$ is

$$\mathbf{A}_{ij} \triangleq \begin{cases} t(i,j) & \text{if } (i,j)\in E_T, \\ \bar{0} & \text{otherwise.} \end{cases}$$

Define $\mathbf{A}^{(k)}$ as $\mathbf{A}^{(k)} \triangleq \bar{\mathbf{1}}\oplus\mathbf{A}\oplus\cdots\oplus\mathbf{A}^k$, where $\mathbf{A}^k \triangleq \mathbf{A}\otimes\mathbf{A}\otimes\cdots\otimes\mathbf{A}$ (k times).

Let $\mathcal{P}(i,j)$, $\mathcal{P}^k(i,j)$ and $\mathcal{P}^{(k)}(i,j)$ be the set of all paths in G_T from i to j, the set of paths from i to j with length k and the set of paths from i to j with length at most k, respectively. Obviously, $\mathcal{P}^k(i,j) \subseteq \mathcal{P}^{(k)}(i,j) \subseteq \mathcal{P}(i,j)$. The following connection between matrix powers and paths of a certain length is well known:

$$\left(\mathbf{A}^k\right)_{ij} = \bigoplus_{p\in\mathcal{P}^k(i,j)} t(p), \tag{1}$$

Note that the proof of (1) relies on the (left) distribution rule. From (1), we directly obtain

$$\left(\mathbf{A}^{(k)}\right)_{ij} = \bigoplus_{p\in\mathcal{P}^{(k)}(i,j)} t(p). \tag{2}$$

If the trust graph $G_T(V,E_T,t)$ is absorptive, then we only need to consider simple paths (i.e., no repetitions of nodes along the path is allowed). In the graph G_T with $|V| = n$, no path length is larger than $n-1$, which means that $\mathcal{P}^{(n-1)}(i,j) = \mathcal{P}(i,j)$. Therefore $\mathbf{A}^{(n-1)} = \mathbf{A}^{(n-1+k)}$ for any $k \geq 0$. From (2), we obtain the solution

$$it(v_i, v_j) = \bigoplus_{p\in\mathcal{P}(i,j)} t(p) = \left(\mathbf{A}^{(n-1)}\right)_{ij}. \tag{3}$$

Many efficient algorithms are available in the literature to compute $\mathbf{A}^k$, see [18]–[21] and the references therein.

2) Eliminating Distributivity: Our way to solve the trust inference problem without distributivity is based on the grouping function g introduced in [22]. The basic idea is that by utilizing the grouping function g, we first convert the problem in a bi-monoid $\mathcal{BM}$ into the problem in a semiring $\mathcal{C}$. Then, we mapping back labels computed in $\mathcal{C}$ to labels in $\mathcal{BM}$.

Let $M(T)$ be the set of all countable multisets that are composed of elements in T. Mathematically the grouping function $g : M(T) \mapsto M(T)$ has the following properties:

1) For $M_1, M_2 \in M(T)$, let $M_1 \otimes M_2$ be the multiset such that $M_1\otimes M_2 \triangleq \{t_1 \otimes t_2 \mid t_1 \in M_1 \text{ and } t_2 \in M_2\}$. Then, $g(M_1 \otimes M_2) = g(g(M_1) \otimes g(M_2))$;
2) For all $M_i \in M(T)$, where $i \in I$ and I is a countable index set, we have $g\left\{\bigcup_{i\in I} M_i\right\} = g\left\{\bigcup_{i\in I} g(M_i)\right\}$;
3) If $M \in M(T)$ then $\oplus(M) = \oplus g(M)$.

Intuitively, if M is a set of path labels, then g groups labels together as long as this does not violate the distributivity. Property 1) states that the grouping process is compatible with $\otimes$, i.e., grouping before a trust evaluation does not change the result of the evaluation. Property 2) requires a natural commutativity property of the grouping process. Finally, Property 3) states that the grouping process is compatible with $\oplus$.

Based on the grouping function g, we can always turn a $\mathcal{BM} = (T, \oplus, \otimes, \bar{0}, \bar{1})$ into $\mathcal{C} = (\hat{T}, \hat{\oplus}, \hat{\otimes}, \bar{0}', \bar{1}')$ as follows:

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

- $\hat{T} \triangleq g(M(T))$;
- $\forall \hat{M}_1, \hat{M}_2 \in \hat{T} : \hat{M}_1 \hat{\otimes} \hat{M}_2 \triangleq g\left(\hat{M}_1 \otimes \hat{M}_2\right)$;
- $\forall \hat{M} \in M(\hat{T}) : \hat{\oplus}\hat{M} \triangleq g\left\{\bigcup \hat{M}\right\}$;
- $\bar{0}' = g(0)$ and $\bar{1}' = g(1)$.

Then, it has been proved in [22] that the solution in $\mathcal{BM}$ is:

$$it(v_i, v_j) = \bigoplus \left(\hat{\bigoplus_{p \in \mathcal{P}(i,j)}} \hat{t}(p) \right) \tag{4}$$

Note that the computation of $\hat{\bigoplus}\hat{t}(p)$ in (4) can be performed like in semirings, i.e. (3).

It is easy to show that the trust inference problem has a solution in $\mathcal{BM}$ if and only if it has a solution in $\mathcal{C}$ defined above and $G_T(V,E_T,\hat{t})$ is absorptive if and only if $G_T(V,E_T,t)$ is absorptive. Therefore, the condition that there exists a solution for $\mathcal{BM}$ is that $G_T(V,E_T,t)$ is absorptive.

IV. Routing Algebra for Uniform Trust Environment

In this section we develop a non-classic routing algebra to study the correctness and optimality of routing protocols under the uniform trust environment, i.e., all nodes in a WANET establish and handle trust in the same way (using the same protocol). We will relax this assumption in Section V.

A. Non-Classic Routing Algebra for Trust-Based Routing

In the physical graph $G_H(V,E_H,h)$, function $h : E_H \mapsto H$ assigns each edge $(i,j) \in E_H$ a physical label $h(i,j) \in H$ describing the physical properties of that link. We define a special physical label $\phi \in H$, corresponding to "no physical link" in G_H. After trust inference process, we can combine the physical graph with the augmented trust graph $G_T^*(V,E,it)$ to obtain the routing graph $G_R(V,E_R,r)$. Then, the main task of trust-based routing is to find a path from each node $v_i \in V - \{v_0\}$ to the destination v_0. In what follows, we develop a non-classical routing algebra to formalize this procedure.

Definition 6: **[Routing Algebra]** Given the routing graph $G_R(V,E_R,r)$, we define the *non-classic routing algebra* over G_R as an algebraic structure $\mathcal{A} = (R, \oplus, \otimes, \bar{0}, \bar{1}, \delta)$, where

- $(R, \oplus, \bar{0})$ is a commutative monoid with $\bar{0}$ as its identity;
- $(R, \otimes, \bar{1})$ is a monoid with $\bar{1}$ as its identity;
- $\oplus$-identity $\bar{0}$ is also an annihilator for $\otimes$;
- $\delta : R \times R \mapsto R$ is a function which combines labels on the *flow graph* of a physical path in G_R into a new one.

Before we proceed, some comments on Def.6 seems in order.

- We should not confuse $\bar{0}$ and $\bar{1}$ in $\mathcal{A}$ with the ones in $\mathcal{BM}$ of Def. 3. Here $\bar{0}$ and $\bar{1}$ are special elements in R, not in T. Also note that the operands of $\oplus$ and $\otimes$ are elements in R, and therefore $\oplus$ and $\otimes$ here may have totally different meanings compared with their counterparts in $\mathcal{BM}$.
- We can also introduce a canonical pre-order $\preccurlyeq_\oplus$ over R, as what we have done for $\mathcal{BM}$. We also denote it as $\preccurlyeq$ for short from now on. $\bar{0}$ is also called *the least preferred label* because $\forall a \in R - \{\bar{0}\} : a \prec \bar{0}$ and $\bar{1}$ is called *the most preferred label* because $\forall a \in R - \{\bar{1}\} : \bar{1} \prec a$.
- Function δ can be interpreted as a combined operator of $\oplus$ and $\otimes$, and its operand is a special structure called flow graph, which will be explained in details as follows.

For a physical path $p_{k,1} = \langle v_k, v_{k-1}, \cdots, v_2, v_1 \rangle$ in G_R, we define the flow graph $\mathcal{F}_{k,1}$ of that path as a labeled directed graph (see Fig. 4 (c) for an illustration) such that

- The vertex set of $\mathcal{F}_{k,1}$ is $V_{1,k} = \{v_1, v_2, \cdots, v_k\}$.

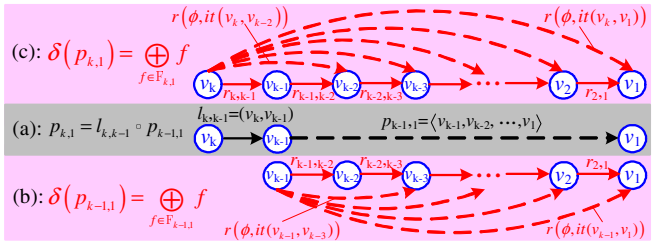


Fig. 4. **Flow graphs, δ function and trust evaluation on paths.**

- The edge set of $F_{k,1}$ is $E_R(\mathcal{F}_{k,1}) \cup E(\mathcal{F}_{k,1})$, where
  - $E_R(\mathcal{F}_{k,1}) \triangleq \{(v_k, v_{k-1}), (v_{k-1}, v_{k-2}), \cdots, (v_2, v_1)\}$ (denoted by solid lines in Fig. 4 (c)).
  - $E(\mathcal{F}_{k,1}) \triangleq \{(v_k, v_{k-2}), (v_k, v_{k-3}), \cdots, (v_k, v_1)\}$ (denoted by dashed lines in Fig. 4 (c)).
- The label on each edge of $\mathcal{F}_{k,1}$ is defined by
  - for edge $(v_i, v_j) \in E_R(\mathcal{F}_{k,1})$, the label will be $r_{i,j}$, i.e., the same as that in the routing graph;
  - for edge $(v_k, v_i) \in E(\mathcal{F}_{k,1})$ $(i = 1, \cdots, k-2)$, the label will be $r(\phi, it(v_k, v_i))$, which is the combination of "no physical link" with the indirect trust $it(v_k, v_i)$ between two nodes.

Obviously, $E_R(\mathcal{F}_{k,1}) \subseteq E_R$ and $E(\mathcal{F}_{k,1}) \subset E$.

Flow graph $\mathcal{F}_{k,1}$ for the physical path $p_{k,1}$ includes all information needed for evaluating the path $p_{k,1}$ from the source node v_k's point of view. It includes the qualities of physical links which consist of path $p_{k,1}$ as well as the trust relationships of the source v_k with intermediate nodes on that path. For traditional routing metrics (i.e., $h(i,j)$ in G_H), a path metric can be simply calculated from the physical link metrics. For example, for path $p_{k,1} = \langle v_k, v_{k-1}, \cdots, v_2, v_1 \rangle$ in G_H, we have $h(p_{k,1}) = h(l_{k,k-1} \circ p_{k-1,1}) = h(l_{k,k-1}) \otimes h(p_{k-1,1})$, where $l_{k,k-1}$ represents link $(k, k-1)$. For trust related metrics, we can observe from Fig. 4 that in general, $\delta(p_{k,1}) = \delta(l_{k,k-1} \circ p_{k-1,1}) \neq \delta(l_{k,k-1}) \otimes \delta(p_{k-1,1})$. However, we can utilize $\mathcal{BM}$ introduced in Section III to calculate $\delta(p_{k,1})$. Note that for flow graph $\mathcal{F}_{k,1}$, $(R, \oplus, \otimes, \bar{0}, \bar{1})$ forms a bi-monoid over R. Let $F_{k,1}$ be the set of all paths from v_k to v_1 in $\mathcal{F}_{k,1}$, $\delta(p_{k,1})$ can be calculated as $\delta(p_{k,1}) = \bigoplus_{f \in F_{k,1}} f$.

B. Conditions for Correct and Optimal Routing

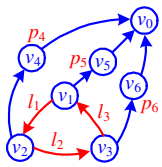
We consider the following properties of function δ, which play an important role in guaranteeing the correctness and optimality of trust-based routing protocols.

Given a routing graph $G_R(V,E_R,r)$, if a path p (or a link l) exists in G_R, we write $p \in G_R$ (or $l \in G_R$) with a slight abuse of notation. We define:

1) Routing algebra $\mathcal{A}$ is *strictly δ-left-monotonic*, if for all link $l \in G_R$ and path $p \in G_R$ satisfying $l \circ p \in G_R$, $\delta(l) \neq \bar{0}$ and $\delta(p) \neq \bar{0}$, we have $\delta(p) \prec \delta(l \circ p)$.
2) Routing algebra $\mathcal{A}$ is *strictly δ-right-monotonic*, if for all link $l \in G_R$ and path $p \in G_R$ satisfying $p \circ l \in G_R$, $\delta(l) \neq \bar{0}$ and $\delta(p) \neq \bar{0}$, we have $\delta(p) \prec \delta(p \circ l)$.
3) Routing algebra $\mathcal{A}$ is *δ-right-isotonic*, if for all link $l \in G_R$ and paths $p, q \in G_R$ satisfying $l \circ p, l \circ q \in G_R$ and $\delta(p) \preccurlyeq \delta(q)$, we have $\delta(l \circ p) \preccurlyeq \delta(l \circ q)$. $\mathcal{A}$ is *strictly δ-right-isotonic* if we replace $\preccurlyeq$ by $\prec$ in above statement.
4) Routing algebra $\mathcal{A}$ is *δ-left-isotonic*, if for all link $l \in G_R$ and paths $p, q \in G_R$ satisfying $p \circ l, q \circ l \in G_R$ and $\delta(p) \preccurlyeq \delta(q)$, we have $\delta(p \circ l) \preccurlyeq \delta(q \circ l)$. $\mathcal{A}$ is *strictly δ-left-isotonic* if we replace $\preccurlyeq$ by $\prec$ in above statement.

Based on the properties we defined for δ function, we can summarize our main results as follows:

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.



(a) Routing graph

	v_0	v_1	v_2	v_3	v_4	v_5	v_6
v_0	--	fr.	fr.	fr.	fr.	fr.	fr.
v_1	fr.	--	fr.	fr.	fr.	st.	en.
v_2	fr.	fr.	--	fr.	st.	en.	fr.
v_3	fr.	fr.	fr.	--	en.	fr.	st.
v_4	fr.	fr.	st.	en.	--	fr.	fr.
v_5	fr.	st.	en.	fr.	fr.	--	fr.
v_6	fr.	en.	fr.	st.	fr.	fr.	--

(b) Trust relationships

For v_1:
$l_1 \circ p_4 \prec p_5 \prec l_1 \circ l_2 \circ p_6$
For v_2:
$l_2 \circ p_6 \prec p_4 \prec l_2 \circ l_3 \circ p_5$
For v_3:
$l_3 \circ p_5 \prec p_6 \prec l_3 \circ l_1 \circ p_4$

(c) v_1-v_3's preferences on paths

Fig. 5. **Example of routing loop in trust-based routing.**

Theorem *1:* A trust-based distance-vector routing protocol is guaranteed to be correct, if an only if (1) the trust graph is absorptive; and (2) routing algebra $\mathcal{A}$ is δ-left-monotonic. A trust-based distance-vector routing protocol is guaranteed to be optimal, if and only if (1) the trust graph is absorptive; and (2) routing algebra $\mathcal{A}$ is δ-left-isotonic and δ-left-monotonic.

Theorem *2:* A trust-based link-state routing protocol is guaranteed to be correct, if an only if (1) the trust graph is absorptive; and (2) routing algebra $\mathcal{A}$ is δ-right-monotonic, δ-right-isotonic and strictly δ-left-isotonic. A trust-based link-state routing protocol is guaranteed to be optimal, if and only if (1) the trust graph is absorptive; and (2) routing algebra $\mathcal{A}$ is δ-right-monotonic, δ-right-isotonic and strictly δ-left-isotonic.

The detailed proofs of these results can be found in our technical report [23]. Here, we just compare our results with Sobrinho's classic routing algebra [11], [12]. Although our results are also characterized by monotonicity and isotonicity of one operator (δ function here), our δ function is totally different with its counterpart (i.e., $\otimes$) in Sobrinho's routing algebra. Our δ function is related to monoid endomorphisms [21], and therefore, is not included in Sobrinho's routing algebra, which is based on ordered semirings.

C. Illustrating Examples

Here, we utilize some concrete examples to explain how to use our abstract results described in previous subsection. We already give an example in Example 1 in Section II-D where the routing protocol is not optimal. It is easy to check that it violates the isotonic property. In what follows, we will give an example which violates the monotonic property.

In Fig. 5, there are three types of trust relationships: friends, strangers and enemies. Fig. 5 (a) gives the routing graph with v_0 as the destination and Fig. 5 (b) represents trust graph in the matrix form. Intuitively, each node will prefer to the most friendly path (we will give the formal definition of this concept a little later). Based on two graphs given in Fig. 5 (a) and (b), for each node v_i, we can rank all possible paths from node v_i to the destination v_0 with order relation $\prec$. Fig. 5 (c) demonstrates path ranking for nodes v_1, v_2 and v_3. Note that trust in this example is non-transitive, which means that a friend's friend is not necessarily also a friend. Therefore, no indirect trust inference phase is needed in this example.

We first demonstrate the way to formalize this problem with the routing algebra proposed in Def. 6. We specify the items in $\mathcal{A}$ as the following:

For the routing algebra $\mathcal{A} = (R, \oplus, \otimes, \bar{0}, \bar{1}, \delta)$, we define

- $R = \{\text{fr., st., en., } \phi\}$ with $\bar{0} = \text{en.}$ and $\bar{1} = \text{fr.}$,
- fr. $\prec$ st. $\prec$ en. $\prec \phi$,
- for all $a, b \in R$, $a \otimes b = \begin{cases} a & \text{when } a \prec b \\ b & \text{when } b \prec a \end{cases}$,
- for all $a, b \in R$, $a \oplus b = \begin{cases} a & \text{when } b \prec a \\ b & \text{when } a \prec b \end{cases}$,
- $\delta : R \times R \mapsto R$ is a function which combines labels on the flow graph of a physical path in G_R into a new one with operators $\otimes$ and $\oplus$ defined above.

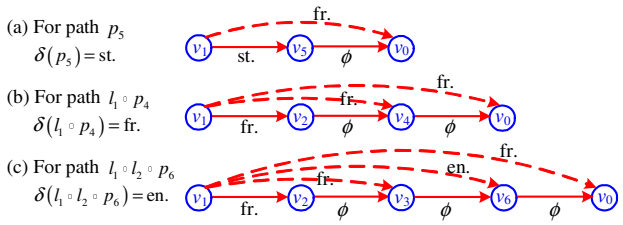


Fig. 6. **Flow graphs for the physical paths from node v_1 to v_0 in Fig. 5.**

Fig. 6 demonstrates flow graphs for three physical paths from node v_1 to the destination v_0 in Fig. 5. Here, we introduce a new label ϕ to indicate the links which will not affect the calculation of the trustworthiness of a path. The intuition here is that the trustworthiness of a path only involves the trust relationships between the source node and intermediate nodes on the path, and depends on the least trustworthy intermediate node. Fig. 7 gives an example of utilizing operators $\otimes$ and $\oplus$ defined above to calculate δ function for the physical path given in Fig. 6 (c).

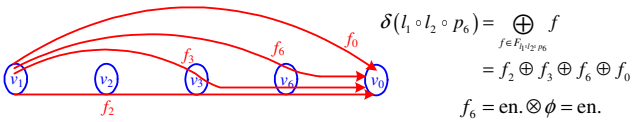


Fig. 7. **Calculating δ function for the physical path given in Fig. 6 (c).**

Obviously, the specification given above leads to the path ranking described in Fig. 5 (c). Our formalization guarantees that for each flow graph $\mathcal{F}$, $(R, \oplus, \otimes, \bar{0}, \bar{1})$ forms a bi-monoid over R. Therefore, we can utilize $\mathcal{BM}$ introduced in Section III to calculate δ functions. Note that, for Sobrinho's classic routing algebra [11], [12], only labels on physical links are involved in the formalization. Therefore, only hop-by-hop trust relationships are included in Sobrinho's classic routing algebra, which are not sufficient for the calculation of the trustworthiness of a whole physical path. It is easy to check that this routing algebra violates the monotonic property, and therefore, it will lead to routing loops. The following analysis will confirm this conclusion.

For link-state routing, the most preferred paths calculated by v_1, v_2 and v_3 are $l_1 \circ p_4$, $l_2 \circ p_6$ and $l_3 \circ p_5$, respectively. Therefore, the next-hop for v_1 is v_2, for v_2 is v_3, and for v_3 is v_1. A loop $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_1$ appears, and packets will be forwarded in this loop forever.

For distance-vector routing, we take v_1 as an example. v_1 has only two choices for the next-hop: v_2 or v_5. In the first choice, we assume that v_1 takes v_2 as the next-hop. Given v_1's choice, v_3 will take v_6 as the next-hop. Given v_3's choice, v_2 will take v_3 as the next-hop. Given v_2's choice, v_1 should take v_5 as the next-hop, because $\delta(p_5) \prec \delta(l_1 \circ l_2 \circ P_6)$. This contradicts to our assumption that v_1 takes v_2 as the next-hop. In the second choice we then assume that v_1 takes v_5 as the next-hop. Given v_1's choice, v_3 will take v_1 as the next-hop. Given v_3's choice, v_2 will take v_4 as the next-hop. Given v_2's choice, v_1 should take v_2 as the next-hop, because $\delta(l_1 \circ p_4) \prec \delta(p_5)$. This contradicts to our assumption that v_1 takes v_5 as the next-hop. As we can observe that in both choices, we all end up with contradictions. Therefore, node v_1 keeps changing its routing table's configuration again and again, no stable status will be achieved. This is called *route oscillation*, another name for *forwarding loop* within distance-vector routing.

For both routing approaches, no in-tree can form and therefore the correctness of routing protocols cannot be guaranteed.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

V. Routing Algebra for Group-Based Trust Environment

A. Motivating Example

Consider a disaster recovery scenario where the local police force may need to coordinate with fire fighters, military forces, and medical crews by sharing information and communicating with each other regardless of the particular networking protocols that each group uses. See Fig. 8 for an illustration.

Obviously, different groups (indicated by different colors in Fig. 8) may have different rules to evaluate and handle trust. Therefore, different trust metrics may be adopted and combined with different trust-based routing protocols. Now node v_1 as a police wants to communicate with node v_0, a doctor, through the most trustworthy path. Multiple questions naturally arise for this task. For example, how does node v_1 evaluate the trustworthiness of path p_1 and p_2, when links along each path are measured by different trust metrics? How to compare p_1 with p_2? What kinds of operation rules do the nodes connecting different groups (like v_3, v_5, v_9 and v_{13} in Fig. 8) need to follow in order to ascertain that there are no loops in hop-by-hop routing? Or under what conditions is the path formed by the next-hop selections of all intermediate nodes the most trustworthy path as defined by the source node v_1? All these questions call for a unified framework to enable the analysis of end-to-end communications over nonuniform WANETs governed by distinct trust metrics.

In this section, we consider a group-based trust environment, where multiple groups coexist in a WANET. Each group i can be modeled as one routing algebra $\mathcal{A}_i = (R_i, \oplus_i, \otimes_i, \bar{0}_i, \bar{1}_i, \delta_i)$ defined in Section IV. The problem here is how to perform end-to-end trust-based routing across multiple groups. To be more focused, we make the following simplifications here:

1) We assume each group is in a uniform trust environment, i.e., there exist uniform rules for the direct trust establishment and indirect trust inference in each group, and these procedures are independent among different groups. Interactions between different groups only happen in the path selection phase.
2) We assume all groups use the same kind of routing protocols, either distance-vector or link-state routing protocols. The problems arise from the inter-operations between two kinds of routing protocols are irrelevant to trust metrics, the theme of this paper.

In previous section, we utilize routing algebra to study the correctness and optimality conditions for trust-based routing in one group. Our key observation here is that the problems involved in multi-group communications are all related to conversions of trust-based routing metrics between different groups. Therefore, based on previous results, the problems of correct and optimal routing in multi-group environment can be more specifically reformulated as the following: what conditions must the conversions between different routing algebra satisfy in order to guarantee the correct and optimal end-to-end trust-based routing?

B. Problem Formalization

We first formalize the notion of conversions between different routing algebras.

***Definition** 7:* **[Conversion Function]** Given $k+1$ routing algebras $\mathcal{A}_i = (R_i, \oplus_i, \otimes_i, \bar{0}_i, \bar{1}_i, \delta_i)$ for $i = 0, 1, \cdots, k$ as defined in Def. 6. Routing algebra $\mathcal{A}_0$ is called the *host algebra*, if all paths across multiple groups will be measured using the labels in R_0. Correspondingly, routing algebra $\mathcal{A}_j$ $(j \neq 0)$ is called the *guest algebra*, since the label of a path p in group $\mathcal{A}_j$ will be converted to that in the host algebra before path p can be utilized by other groups. We define two *conversion functions* between $\mathcal{A}_0$ and $\mathcal{A}_j$ as:

(1) $\beta_{0\to j} : R_0 \mapsto R_j$; (2) $\beta_{j\to 0} : R_j \mapsto R_0$.

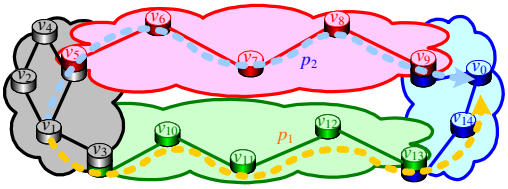


Fig. 8. **Trust-based routing across multiple groups.**

Next, we show how to model basic inter-operations between host algebra / group $\mathcal{A}_0$ and guest algebra $\mathcal{A}_1$ by utilizing conversion functions. We only consider two groups here. It is straightforward to extend our discussion to more groups. Refer to Fig. 9 for an illustration. Here, node v_m belongs to both groups, and acts as bridge router to connect two groups. Node v_m finds a path, say $p_{m,1}$, to the designation node v_1 in group $\mathcal{A}_1$. Let the label calculated by v_m for path $p_{m,1}$ be $\delta_1(p_{m,1})$. In the distance-vector routing, node v_m needs to advertise the information about path $p_{m,1}$ to its neighbor, say v_{m+1} in group $\mathcal{A}_0$. The label $\delta_1(p_{m,1})$ cannot be directly used because for v_{m+1} label $\delta_1(p_{m,1})$ belongs to different trust metric set R_1, which cannot be understood and further processed by v_{m+1}. Therefore, v_m need first convert $\delta_1(p_{m,1})$ into $\beta_{1\to 0}(\delta_1(p_{m,1}))$, i.e., the trust metric used in R_0. Note that, we assume the trust inference process is performed in each group independently. Therefore, node v_{m+1} has no indirect relationships with nodes in group $\mathcal{A}_1$ except v_m. The label of path $p_{m+1,1} = (v_{m+1}, v_m) \circ p_{m,1}$ can be simply calculated as $\delta_0(p_{m+1,1}) = r_{m+1,m} \otimes_0 \beta_{1\to 0}(\delta_1(p_{m,1}))$, where $r_{m+1,m} \in R_0$ is the label of link (v_{m+1}, v_m). For link-state routing, source node v_k need calculate the label (i.e., trust metric) $\delta_0(p_{k,1}) \in R_0$ for the whole path $p_{k,1} = p_{k,m} \circ p_{m,1}$. This path can be separated into two parts: subpath $p_{k,m}$ with label $\delta_0(p_{k,m}) \in R_0$ and subpath $p_{m,1}$ with label $\delta_1(p_{m,1}) \in R_1$. Since two labels belong to different trust metric sets, they cannot be directly compared or combined. By utilizing $\beta_{1\to 0}$, we can simply compute $\delta_0(p_{k,1}) = \delta_0(p_{k,m}) \otimes_0 \beta_{1\to 0}(\delta_1(p_{m,1}))$.

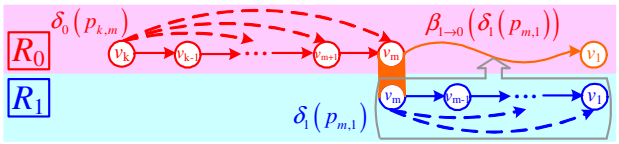


Fig. 9. **Concatenation of paths from different groups.**

Two important observations can be made through this example. (1) Although there are three operations defined in each routing algebra $\mathcal{A}_i$, i.e., $\oplus_i$, $\otimes_i$ and δ_i, only $\otimes_i$ involves in path label calculations across multiple groups. Therefore, the interactions between conversion functions and $\otimes_i$ operators will play a key role to determine the properties of the whole system (with multiple groups). (2) If we abstract each path contained in one group (like paths $p_{k,m}$ and $p_{m,1}$ in Fig. 9) as a generalized link, from the view point of group $\mathcal{A}_0$, conversion function $\beta_{1\to 0}$ assigns each generalized link from other groups a new (generalized) link label. The principles established for one group obviously apply here. Conversion functions can not be arbitrary: in order to guarantee the correctness and optimality of trust-based routing across multiple groups, some constraints on them must be imposed. To characterize those constraints is what we will do next.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

C. Conditions for Correct and Optimal Routing

Conversion function pair $(\beta_{j\to 0}, \beta_{0\to j})$ represents relationships between host algebra $\mathcal{A}_0$ and guest algebra A_j. Here we first consider the following properties of conversion function pair, which will be used to analyze the correctness and optimality of trust-based routing across multiple groups. Recall that for every routing algebra $\mathcal{A}_i$, a canonical pre-order $\preccurlyeq_i$ can be naturally introduced from $\oplus_i$. We define:

(1) Function pair $(\beta_{j\to 0}, \beta_{0\to j})$ is *guest-order-preserved* if
- $\forall r_a, r_b \in R_0$, if $r_a \preccurlyeq_0 r_b$ we have $\beta_{0\to j}(r_a) \preccurlyeq_j \beta_{0\to j}(r_b)$.

(2) Function pair $(\beta_{j\to 0}, \beta_{0\to j})$ is *host-order-preserved* if
- $\forall r_a, r_b \in R_j$, if $r_a \prec_j r_b$ we have $\beta_{j\to 0}(r_a) \prec_0 \beta_{j\to 0}(r_b)$.
- $\forall r \in R_0, r \preccurlyeq_0 \beta_{j\to 0}(\beta_{0\to j}(r))$.

(3) Function pair $(\beta_{j\to 0}, \beta_{0\to j})$ *distributes* over $\otimes$ if
- $\beta_{j\to 0}$ is bijective and $\beta_{0\to j} = \beta_{j\to 0}^{-1}$,
- $\forall r_a, r_b \in R_j$, $\beta_{j\to 0}(r_a \otimes_j r_b) = \beta_{j\to 0}(r_a) \otimes_0 \beta_{j\to 0}(r_b)$.
- $\forall r_a, r_b \in R_0$, $\beta_{0\to j}(r_a \otimes_0 r_b) = \beta_{0\to j}(r_a) \otimes_j \beta_{0\to j}(r_b)$.

To facilitate our analysis, we define a universal routing algebra $\mathcal{A} = (R, \oplus, \otimes, \bar{0}, \bar{1}, \delta, \preccurlyeq)$ upon $\mathcal{A}_0$ and $\mathcal{A}_j$, where
- $R = R_0 \cup R_1 \cup \cdots \cup R_k$
- $\otimes : R \times R \mapsto R$ is a function such that $\forall a \in R_i, b \in R_j$:

$$a \otimes b \triangleq \begin{cases} a \otimes_j b & \text{if } i = j, \\ \beta_{i\to j}(a) \otimes_j b & \text{otherwise.} \end{cases}$$

As we discussed before, $\oplus_i$ and δ_i never involved in path calculations across multiple groups, which means operands of $\oplus$ or δ are always the same. Therefore, we define:
- $a \oplus b = a \oplus_i b$ if $a, b \in R_i$,
- $\delta(p) = \delta_i(p)$ if the whole path p is in group $\mathcal{A}_i$.

For $\mathcal{A}$, $\preccurlyeq$ cannot be introduced from $\oplus$, and therefore should be defined independently:
- $\preccurlyeq$ is an order relation over R such that $\forall a \in R_i, b \in R_j$:

$$a \preccurlyeq b \triangleq \begin{cases} a \preccurlyeq_j b & \text{if } i = j, \\ \beta_{i\to 0}(a) \preccurlyeq_0 \beta_{j\to 0}(b) & \text{otherwise.} \end{cases}$$

Given $\preccurlyeq$, $\bar{0}$ and $\bar{1}$ is defined as follows:
- $\bar{0} \in R$ such that $\forall a \in R - \{\bar{0}\}, a \prec \bar{0}$,
- $\bar{1} \in R$ such that $\forall a \in R - \{\bar{1}\}, \bar{1} \prec a$.

Based on above discussions, we have the following results:

Lemma *1:* Order relation $\preccurlyeq$ defined in universal routing algebra $\mathcal{A}$ is a total pre-order over R if all pairs $(\beta_{j\to 0}, \beta_{0\to j})$ are host-order-preserved.

In the universal routing algebra $\mathcal{A}$, the correctness and optimality conditions for R and $\otimes_0$ can be transformed to that for conversion functions, $\otimes_i$ and R_i. Utilizing the properties of conversion functions characterized above, we can obtain the following results.

Theorem *3:* Given $k+1$ routing algebras $\mathcal{A}_i$ $(i = 0, \cdots, k)$ and conversion function pairs $(\beta_{j\to 0}, \beta_{0\to j})$ $(j = 1, \cdots, k)$, a distance-vector routing protocol $\mathcal{R}$ is guaranteed to be correct across multiple groups if (1) $\mathcal{R}$ is correct in each routing algebra; and (2) all pairs $(\beta_{j\to 0}, \beta_{0\to j})$ are host-order-preserved. A distance-vector routing protocol $\mathcal{R}$ is guaranteed to be optimal across multiple groups if (1) $\mathcal{R}$ is optimal in each routing algebra; and (2) all pairs $(\beta_{j\to 0}, \beta_{0\to j})$ are host-order-preserved and guest-order-preserved.

Theorem *4:* Given $k+1$ routing algebras $\mathcal{A}_i$ $(i = 0, \cdots, k)$ and conversion function pairs $(\beta_{j\to 0}, \beta_{0\to j})$ $(j = 1, \cdots, k)$, a link-state routing protocol $\mathcal{R}$ is guaranteed to be correct and optimal across multiple groups if (1) $\mathcal{R}$ is correct and optimal in each routing algebra; and (2) all pairs $(\beta_{j\to 0}, \beta_{0\to j})$ are host-order-preserved, guest-order-preserved and distributive.

Due to space constraints, detailed proofs of above results are omitted here and can be found in our technical report [23].

VI. Concluding Remarks

In this paper, we develop a formal framework and theory to investigate the correctness, optimality, inter-operativity of trust-based routing protocols for WANETs. Our results obtained here can be extended in two ways. (1) For indirect trust inference problems, we only consider the situation when all trusts in a WANET are transitive. When transitive and non-transitive trust coexist in a WANET, a new algebraic structure for a combined trust metric is needed and consequently new algorithm should be designed to infer indirect trust under non-transitive trust constraints. (2) From routing's point of view, in our framework we only consider topology-based routing protocols. We can extend our study to location-based routing like geographic routing, which is popular for WANETs. Also in this paper we restrict ourselves to unicast routing. Obviously, the trust metrics for multicast, broadcast, and anycast are totally different from that for unicast, and the concept of path selection will be replaced by tree selection. Therefore, these topics should be further investigated.

References

[1] C. Perkins, *Ad Hoc Networking*. Addison Wesley Professional, 2000.
[2] J. Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobile ad hoc networks," in *Proc. of MobiHoc 2001*, Long Beach, CA, Oct. 2001.
[3] L. Buttyan and J.-P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, UK: Cambridge University Press, 2007.
[4] S. Capkun, L. Buttyan, and J. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52–64, Jan. 2003.
[5] C. Zhang, Y. Song, and Y. Fang, "Modeling secure connectivity of self-organized wireless ad hoc networks," in *Proc. of InfoCom 2008*, Phoenix, AZ, April 2008.
[6] Y.-L. Sun, W. Yu, Z. Han, and K. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305–317, Feb. 2006.
[7] F. Oliviero and S. Romano, "A reputation-based metric for secure routing in wireless mesh networks," in *Proc. of IEEE GLOBECOM 2008*, New Orleans, LA, Dec. 2008.
[8] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318–328, Feb. 2006.
[9] A. Jøsang, "An algebra for assessing trust in certification chains," in *Proc. of NDSS'99*, San Diego, CA, Feb. 1999.
[10] M. Yu and K. Leung, "A trustworthiness-based qos routing protocol for wireless ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1888–1898, April 2009.
[11] J. L. Sobrinho, "Algebra and algorithms for qos path computation and hop-by-hop routing in the internet," *IEEE/ACM Transactions on Networking*, vol. 10, no. 4, pp. 541–550, August 2002.
[12] ——, "An algebraic theory of dynamic network routing," *IEEE/ACM Transactions on Networking*, vol. 13, no. 5, pp. 1160–1173, Oct. 2005.
[13] Y. Yang and J. Wang, "Design guidelines for routing metrics in multihop wireless networks," in *Proc. of InfoCom 2008*, Phoenix, AZ, April 2008.
[14] M. Lu and J. Wu, "Opportunistic routing algebra and its applications," in *Proc. of InfoCom 2009*, Rio de Janeiro, Brazil, April 2009.
[15] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. of MobiCom 2000*, Boston, USA, August 2000.
[16] S. Capkun, J. Hubaux, and L. Buttyan, "Mobility helps security in ad hoc networks," in *Proc. of MobiHoc 2003*, Annapolis, MD, June 2003.
[17] J. Golbeck, *Trust on the World Wide Web: A survey*. Delft, The Netherlands: Now Publishers, 2006.
[18] B. Carré, *Graphs and Networks*. Oxford University Press, 1979.
[19] M. Gondran and M. Minoux, *Graphs and Algorithms*. Chichester: Addison Welsey, 1984.
[20] M. Mohri, "Semiring frameworks and algorithms for shortest-distance problems," *Journal of Automata, Languages and Combinatorics*, vol. 7, no. 3, pp. 321–350, 2002.
[21] M. Gondran and M. Minoux, *Graphs, Dioids, and Semirings: New Models and Algorithms*. Springer, 2008.
[22] T. Lengauer and D. Theune, "Unstructured path problems and the making of semirings," in *Proc. of Algorithms and Data Structures: 2nd Workshop, WADS'91*, Ottawa, Canada, Aug. 1991.
[23] C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trust-based routing in wireless ad hoc networks," Technical Report, May 2009. [Online]. Available: http://winet.ece.ufl.edu/~czhang/