2012 American Control Conference
Fairmont Queen Elizabeth, Montréal, Canada
June 27-June 29, 2012

Composite Trust in Networked Multi-Agent Systems

John S. Baras, and Tao Jiang

Abstract–**Trust plays a crucial role in the analysis, synthesis and operation of the integrated system consisting of social-cognitive, information and communication networks. Multi-agent systems and associated coalition operations, which involve two or more organizations, further augment the diversity and complexity of network interactions. Trust and its derivative notions affect dramatically the networked coalition operations. A substantial part of the research challenge has to do with the multitude of meanings, interpretations, symbolisms and mathematical models used to represent and analyze trust. In this paper, we introduce value directed graphs with weighted nodes as our model for composite trust. We extend the value directed graph with weighted nodes composite trust model to include not only numerical weights, but also constraints. We show that the semiring-based constraint satisfaction problem (SCSPs) framework can serve as the unified model to investigate trust relation establishment.**

I. INTRODUCTION

As civilian and military organizations are transforming themselves into enterprises capable of network-centric operations (NCO), they remarkably rely on a diverse set of complex systems that depend on interacting networks in the communications, information, and social-cognitive domains. Multi-agent systems and associated coalition operations, which involve two or more organizations, further augment the diversity and complexity of network interactions. These two types of heterogeneity create new and fundamental challenges related to the interoperability of networks that belong to different domains and different organizations.

Future networked multi-agent systems will be dynamic, in the sense that their coalition structure, information availability, communication connectivity will vary with time at various time scales. Realizing this potential requires resolving many research challenges since these networks need to self-organize, operate in a distributed and asynchronous fashion, and be robust with respect to various changes, failures and adversaries in the networked system. The dynamic nature of future networks and coalition formations pose substantial difficulties in using traditional security mechanisms, such as those involving cryptography and access control (Lampson, Abadi, Burrows, & Wobber, 1991). It is widely believed that such security difficulties can be mitigated through efficient trust management systems.

Trust and its derivative notions affect dramatically the networked coalition operations of any network in each domain (i.e. communication, information, social-cognitive), and even further the networked system consisting of dynamically interacting networks from each domain. As a consequence, it is not enough to analyze models of trust based on *individual* (equivalently *local*) and *global* network parameters within a domain, as is done in current research on trust in various fields, such as social networks (Buskens, 2002), information networks (Bloch, 1996) and communication networks . Rather, we must develop models and methodologies that can represent and analyze the effects of trust *across domains*, i.e. across the different types of interacting networks and organizations. A substantial part of the research challenge has to do with the multitude of meanings, interpretations, symbolisms and mathematical models used to represent and analyze trust and its consequences. For example, as was shown in our recent work (Baras, Jiang, & Purkayastha, 2008), one can analyze jointly the effects of trust coming from a social network perspective, on a communication network (supporting the social network) performance, by using trust related weights on the nodes, and by extending the recently developed network utility maximization (NUM) approach (Chiang, Low, Calderbank, & Doyle, 2007) to systematically develop cross-domain design of high performance communication network protocols that are security or trust aware. In this paper, we introduce the *value directed graph with weighted nodes* as our model for composite trust. We extend the composite trust model to include not only numerical weights, but also constraints. We show that the semiring-based constraint satisfaction problem (SCSPs, (Bistarelli, 2004)) framework can serve as the unified model to investigate trust relations establishment.

In the rest of this paper, we will describe the challenges of trust management that are unique for networked systems and coalition operations. Then we will introduce trust models and methodologies we believe to be suitable in such highly heterogeneous systems.

II. TRUST MANAGEMENT IN NETWORKED MULTI-AGENT SYSTEMS

A. *Composite Trust*

Trust, as a composite concept, consists of components that are derived from different network environments (such as social-cognitive, information and communication networks). Trust in social-cognitive networks must account for the complex interactions and behaviors of humans, capable to represent the way trust is generated and maintained in human organizations, as well as the uncertain and dynamic character of trust as a result of the inherent dynamics and autonomy in human decision making. Trust in information networks must account for the representation and effects of trust in the collection of data, in the processing of data to derive

J.S. Baras, is with the Institute for Systems Research, University of Maryland, College Park, MD 20742, USA (phone: 301-405-6606; fax: 301-314-9218; e-mail: baras@umd.edu).

T. Jiang, was with the Institute for Systems Research, University of Maryland, College Park, MD 20742, USA. She is now with Intelligent Automation Inc., Rockville, MD, USA (e-mail: tjiang@umd.edu).

978-1-4577-1094-0/12/$26.00 ©2012 AACC

information-knowledge-models, in the distribution of data-information-knowledge. Trust in communication networks must encompass representations of trust in the various physical and software entities involved in the communication network, in the operation of the communication network and in its connectivity. Therefore, trust appears in networked multi-agent systems in various ways and meanings. For instance, one can refer to the reduced trustworthiness of a portable device, meaning that the device may have been compromised. Or one refers to the trustworthiness of the data transmitted by a communication device. Or one can refer to a compromised link due to jamming, which reduces the trustworthiness of the link. Thus, trust consisting of collaborating humans and automated agents (sensors, actuators, and computers) is a *composite entity*, represented by several metrics and/or parameters. Clearly there are numerous couplings in these notions of trust. It is not enough to analyze models of trust based on an individual network environment. Rather, we must develop models and methodologies that can represent and analyze the effects of trust across various networked environments. Trust, in any of its forms and representations, affects dramatically the performance of any networked environment.

The primary goal of trust management in such composite environments is to develop useful abstractions and models for trust, that can be appropriately modified and tuned to fit current interpretations of trust in each of the network types present in the overall system, while at the same time can be substantially extended to efficiently capture the interactions between the various networks and integrated into a *composite trust* view of the entire system.

Furthermore, consider a coalition such as the one in Fig.1

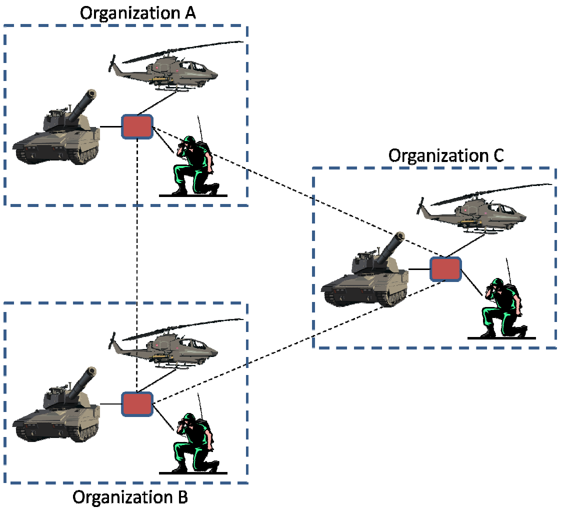

Fig. 1. Networked Coalition Operations

Agents from different organizations must build up trust between each other before conducting operations within the coalition. Coalition operations have to deal with differences among organizations. Such differences exist across all network domains. For instance, participants of each organization may have different views of trust that are influenced by their mission and organization policies. The trust related information collected by one organization may not satisfy the needs of another organization. The protocols regarding transmission of trust evidence may be different in each organization. Therefore, trust management using numerical trust metrics is not applicable within the context of multi-agent and coalition operations. Instead, trust management in multi-agent and coalition operations should identify mutual interests, establish operational requirements and benefits, and eventually establish trust between organizations (Agrawal, Chivers, Clark, Jutla, & McDermid, 2008). Therefore, trust management should also be able to incorporate trust policies rather than just numerical trust evaluation.

B. *Components of Trust Management*

Trust management is to collect, analyze and present trust related evidence and to make assessments and decisions regarding trust relationships between entities in a network (Blaze, Feigenbaum, & Lacy, 1996). Figure 2 describes components of a trust management system in dynamic networks and their interactions.

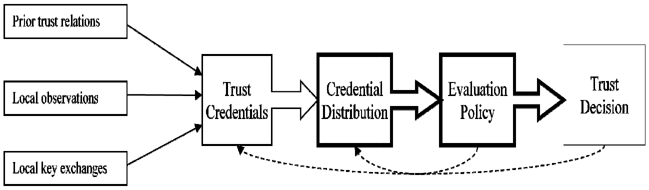

Fig. 2. Trust Management System in Dynamic Networks

In multi-agent systems, trust credentials that are used as evidence for trust evaluation are created and stored distributedly in the network. A trustor usually has to contact agents in different domains to obtain necessary trust credentials. Due to the differences among domains, such a credential distribution process requires a negotiation process that includes identifying required credentials, locating credentials and formatting credentials in the way that can be securely transmitted across networks and understood by the trustor. After distributing trust credentials, the next step is to correctly evaluate trustworthiness of the target given these credentials. Our previous research has extensively studied both trust credential distribution and evaluation of trust, such as (Jiang & Baras, 2008; Jiang & Baras, 2006).

III. EXTENDED VALUE DIRECTED GRAPHS

A crucial component of a trust management system is to provide trust metrics -- a measurable indicator of trust among agents. In our trust framework, we introduce *value directed multi-graphs with weighted nodes* to represent the composite trust. This model is inspired by advanced dynamic network models and trust research in social networks (Buskens, 2002). Value Directed Graphs with Weighted Nodes (VADIGWEN) (Buskens, 2002) are directed graphs with weights on their links and nodes. The graphs are relational, i.e. they represent relations between the nodes (e.g. organizational, social relations). These weights W_{ij}, W_i in the context of trust in social networks represent the strength of a relation that exists between node i and j, or the importance of a node i, respectively. In our model, each network (such as social-cognitive, information, communication network) is modeled by a value directed graph with weighted nodes as illustrated in Figure 3.

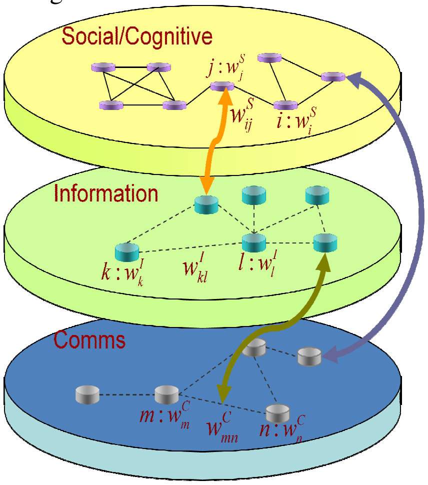

Fig. 3. Value directed multi-graphs with weighted nodes

The superscript in each weight designates the domain: W_{ij}^S, W_i^S, for social/cognitive networks, W_{ij}^I, W_i^I, for information networks W_{ij}^C, W_i^C, for communication networks. Now, in this cross-network context a graph can represent a physical relation (in addition to a logical relation); e.g. connectivity or interference in a communication network. Furthermore, as illustrated in Figure 3, there are relations and constraints across the three domains, indicating the interactions between the graphs. We call the resulting model *Value Directed Multi-Graphs with Weighted Nodes* (VADIMGWEN).

Even within each domain network we encounter many situations that call for multiple metrics; e.g. benefits from collaboration *vs.* trust in social networks (Baras & Jiang, 2005), decision making performance *vs.* time latency required to assess trust *vs.* confidence in trust information in social networks. Thus we are naturally led to investigate models consisting of directed graphs with vector weights on their links and nodes. We call the resulting model *Multi-value Directed Graphs with Weighted Nodes*, or simply *Multi-value Weighted Directed Graphs* (MVAWDIG). When we use such a model for each domain network, we are naturally led to a model of great interest and promise that we call *Multi-value Weighted Directed Multi-Graph* (MVAWDIMG).

There are various ways to numerically represent trust weights. In some trust schemes, continuous or discrete numerical values are assigned to measure the level of trustworthiness. For example, in (Maurer, 1996), an entities opinion about the trustworthiness of a certificate is described by a continuous value in [0, 1]. In (Theodorakopoulos & Baras, 2006), a 2-tuple in $[0; 1]^2$ describes the trust opinion. In (Josang A. , 2001), the metric is a triplet in $[0; 1]^3$, where the elements in the triplet represent belief, disbelief, and uncertainty, respectively. Trust can also be interpreted as probability. In (Josang & Ismail, 2002), subjective probability is defined, while objective probability is used in (Kamvar, Schlosser, & Garcia-Molina, 2003). As a concept of uncertainty, entropy in information theory is a natural measurement of trust as well (Sun, Han, Yu, & Liu, 2006). In the extreme case, trust can be binary: *trust* (trust weight = 1) or *distrust* (trust weight = 0) because either there is 100% security in the network or the approach to evaluate trust is very coarse. There is no absolutely right or wrong for these representations. All the aforementioned numerical representations are suitable for different environments and management requirements.

As we discussed before, in the context of networked multi-agent systems, the trust weight on a node or an arc cannot be simply represented by values. We propose to develop more sophisticated models for composite trust and trust metrics, for several reasons. For example we should not use only values to capture the level of confidence the trustor has on the trustee. Many other social/cognitive/behavioral factors have impacts on decisions, such as the trustor's inclination to take risks, the trustor's and trustee's position in the network, the trustor's access to information and situation awareness, the degree of tolerance of potential disappointment, or the amount of returns yielded through consequent actions, the trustor's evaluation of risk, etc. generally, the enabling/constraining aspects of structural context. Furthermore, the inherent constraints and policies imposed by social exchange, information aggregation and physical communications add more dimensions to the representation of trust and require the modeling of trust to go beyond numerical weights-based metrics. For example, the organizational structure may constraint the process of trust data collection (e.g. legitimate data locations) and thus impacts the level of trust an agent derives based on the available data, or two agents, that highly trust each other, fail to cooperate due to disconnection in the communication network. Therefore, the trust weights should be a mathematical structure that includes logical variables in the form of *constraints*. This allows incorporation of rule-based and behavioral models, social interaction protocols, knowledge model constraints, cross-network constraints and requirements. The resulting models, now involve multi-graphs, with links and nodes annotated by mixtures of numerical and logical variables. We call such models *extended value directed graphs*. Elements of each trust weight structure represent trust from various contexts. Different types of representations can be used to satisfy the requirements in each element's context. For example, in social-cognitive networks, subjective probability can be used to model human beings' perception on trust (Gambetta, 1988); many inherent constraints and policies imposed by social exchange, information aggregation and physical communications can only be represented using logical structures in the form of constraints.

IV. EVALUATION OF COMPOSITE TRUST

The evaluation of the composite trust structure using *extended value directed graphs* requires a general algebraic structure. We present our trust evaluation model that uses the mathematics of partially ordered semirings (Baccelli, Cohen, Olsder, & Quadrat, 1992). Remarkably not only have we been able to apply these mathematical methods to practical problems (Theodorakopoulos & Baras, 2006), but in addition they are very similar to performance analysis tools like Network Calculus (LeBoudec & Thiran, 2004). The fact that ordered semirings provide the foundation for handling constraints and constrained based reasoning (Bistarelli, 2004) provides the foundation for evaluation of composite trust in the extended value directed graphs.

We first briefly describe constraint based reasoning based on partially ordered semirings. Constraint solving has been an active area of research in AI. A Constraint Satisfaction Problem ((CSP), (Russell & Norvig, 1995)) consists of a set of problem variables, a domain of possible values for each variable, and a set of constraints, each of which specifies an acceptable combination of values for one or more of the problem variables. Therefore in a CSP, each constraint is simply a set of tuples over some subset of the problem variables. A solution for a CSP is an assignment of values to the variables that satisfies all the constraints of the problem.

The constraints we are particularly interested in are *soft constraints*, which express preferences, or prioritized constraints. Given soft constraints, certain less preferred constraints can be sacrificed if the solution is good enough with regard to some other criterion. This is particularly useful for networked multi-agent systems. Each domain defines its own constraints. Without global coordination, the constraints from different domains may turn out to be in conflict with each other. If the system insists on solving the constrained based problem (trust evaluation in the context of this paper) that satisfies all the constraints given some are in conflict, the solution set is obviously empty. Then as a result, no operations can be conducted because agents of different domains fail to establish trust between each other.

CSPs cannot efficiently model soft constraints or model partial knowledge. Therefore, semiring-based CSPs (SCSPs, (Bistarelli, 2004)) are proposed to address the above shortcomings of CSPs. A *semiring* is a tuple $< A, +, \times, \mathbf{0}, \mathbf{1} >$ where

- A is a set with $\mathbf{0}, \mathbf{1} \in A$;
- $+$, the additive operation, is closed, commutative and associated over A with $\mathbf{0}$ as its identity element;
- $\times$, the multiplicative operation, is closed and associative over A with $\mathbf{1}$ as its identity element and $\mathbf{0}$ as its absorbing element;
- $\times$ distributes over $+$.

A *c-semiring* (or constraint semiring) is a semiring such that $+$ is idempotent, $\times$ is commutative, and $\mathbf{1}$ is the absorbing element of $+$. The $+$ operation of a c-semiring then naturally defines a partial order over the elements of the semiring; if $S = < A, +, \times, \mathbf{0}, \mathbf{1} >$ is a *c*-semiring with $a, b \in A$ and $a + b = b$ then we say that $a \leq_S b$, which means that b is better than a under this partial order over S. It is easily shown that both $+$ and $\times$ are monotone in the ordering $\leq_S$. An *lc*-semiring is a *c*-semiring for which A is finite and the $\times$ operation is idempotent.

A semiring-based constraint system is a tuple $< S, D, V >$ where S is a semiring, D is a finite set and V is an ordered set of variables. A constraint over such a system is a tuple $< def, con >$ where $con \subseteq V$ is known as the type of the constraint, and $def: D^k \to A$ (where k is the cardinality of V) is the value of the constraint. Thus def assigns a value from the semiring to each combination of values of the variables on con. This value can be interpreted as strength of preference, a probability, a cost, or something else depending on the problem. An SCSP is then a tuple $< C, v >$ where $v \subseteq V$ and C is a set of constraints.

The solution of an SCSP is the constraint obtained by combining all the constraints in the SCSP and projecting it over the set v of variables of interest. The best level of consistency (*blevel*) of the SCSP is the projection of the solution over the empty set. Thus the *blevel* represents the highest valuation that can be attained by a tuple under the constraints. In other words, the *blevel* gives the maximum extent to which a given set of constraints can be satisfied. Finding the best level of consistency is an NP-complete problem, as is solving the SCSP. However, many special cases can be solved efficiently. For an *lc*-semiring, local consistency algorithms yield approximate solutions efficiently (Bistarelli, 2004). In some special cases (where $\times$ is not necessarily idempotent), dynamic programming yields a solution in $O(n)$ time (Bistarelli, 2004). SCSPs have also been used in a variety of applications. For instance, Bella and Bistarelli (Bistarelli, 2004) used them to model the Needham-Schroeder protocol and showed that the model can be used to "discover" a well-known attack on this protocol.

The natural choice for the semiring we define in the SCSP of trust evaluation is the Trust Semiring. The previous work by one of the authors (Theodorakopoulos & Baras, 2006) demonstrated the trust semiring on single graphs. This definition of the trust semiring can be easily extended to the value directed multi-graphs with weighted nodes for composite trust. We define W as the trust weight space. If the trust weight is a continuous value ranging from 0 to 1, such as the trust weights used in (Maurer, 1996), W is $[0,1]$. If we consider the trust weight as a two-dimensional vector as in (Theodorakopoulos & Baras, 2006), W is $[0,1]^2$. W can also be a finite set. For instance, in PGP (Zimmermann, 1995), S={"unknown," "untrusted," "marginally trusted," "fully trusted"}. W can also be the product of multiple spaces that represent different types of trust metrics in different domains. Based on intuitive concepts about trust evaluation in a network, we can expect the binary operators to have the following properties in addition to those required by the semiring structure:

- Since trust should deteriorate along a path, we require the following for the $\times_{trust}$ operator:
$$a \times_{trust} b \leq_S a, b \quad \text{given } a, b \in W$$
where $\leq_S$ is the partial order over S defined above. Note that the total trust along a path is "limited" by the source's trust for the first node in the path.
- Regarding aggregation across paths with the $+_{trust}$ operator, we generally expect that trust quality will improve, since we have multiple opinions. In a fashion similar to the $\times_{trust}$ operator, we require that the $+$ operator satisfies:
$$a +_{trust} b \geq_S a, b.$$
- The $\mathbf{0}$ element (identity element for $+_{trust}$, absorbing for $\times_{trust}$) corresponds to the opinion "I don't know" (*not* the most negative opinion). This

corresponds to nonexistent trust relations between nodes. The rationale is that if a **0** is encountered along a path, then the whole path "through" this opinion should have weight equal to **0**. Also, such opinions should be ignored in $+_{trust}$.

- The element **1** (identity element for $\times_{trust}$) is the "best" trust weight that can be assigned to a node. This can also be seen as the trust of a node about itself.

One example of the trust semiring is *TS* = $<[0,1], \max, \min, 0, 1>$. It is easy to check that *TS* satisfies the above properties. In fact, *TS* is a *c*-semiring as we show below.

Theorem 1 The trust semiring *TS* = $<[0,1], \max, \min, 0, 1>$ is a *c*-semiring.

Proof: The + operator is idempotent, because $\max(a, a) = a$. The × is commutative as $\min(a, b) = \min(b, a)$. 1 is the absorbing element of + because $\max(1, a) = 1$. Therefore, *TS* is a *c*-semiring. ■

The trust weights evolve while the trust evaluation proceeds. We define two rules for trust evaluation:

- *Concatenation*: given W_{ij} and W_{jk}, we have that $W_{ik} = W_{ij} \times_{trust} W_{jk}$.
- *Aggregation*: given W_{ij}, W_{ih}, W_{jk} and W_{hk}, $W_{ik} = W_{ij} \times_{trust} W_{jk} +_{trust} W_{ih} \times_{trust} W_{hk}$.

Using the trust semiring, we can define the *trust constraint system*, which represents the network (or networked system) on which the trust evaluation process is executed. Next, we will describe the development of trust evaluation with constraints and give a detailed formulation of the trust SCSP for a specific scenario.

V. CONSTRAINT PROGRAMMING FOR TRUST EVALUATION

The central idea is that the constraints regarding evaluating trustworthiness of agents in a networked multi-agent system can be written as a set of constraints in the SCSP framework. We first define the *initial SCSP*, which specifies the trust weights when dynamic trust evaluation has not yet started. These trust weights are called the "direct trust weights". Direct trust comes from previous interactions between the trustor and the trustee, local observations from the trustor on the trustee, or verified certificates regarding the trustee. In our proposed framework, the direct trust is represented as an element in the trust semiring *TS*.

As we discussed before, the trust in networked multi-agent systems should take various constraints into consideration. These constraints are written in the form of constraints in the SCSP framework. In general, the procedure for formulating and solving the trust SCSP is as follows:

- Choose an appropriate trust semiring.
- Collect all the constraints and represent them as constraints over the chosen semiring.
- Run certain solvers to obtain the solution of the trust SCSP.

Now we present a specific example to illustrate the main idea. Figure 4 is an example of a multi-graph with weights on trust, where two levels of trust graphs represent trust relations of two different domains, such as information and communication domains. The goal is to evaluate trust between node A and node D given direct trust relations from two domains.

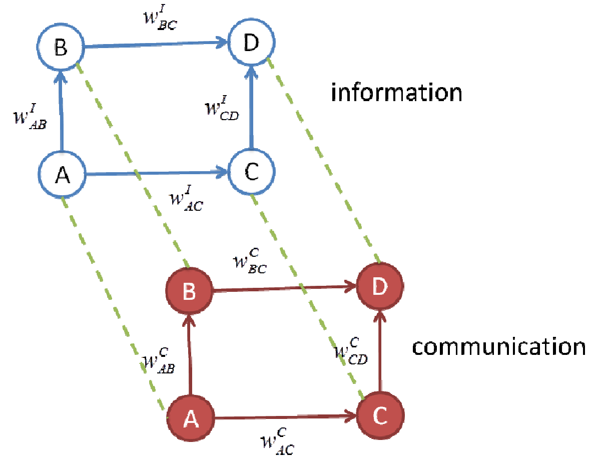

Fig. 4. Example of a two-level graphs with trust weights

Suppose the information trust between nodes k and l is denoted as $w^I_{kl} \in W^I$, where W^I can be any trust weight space mentioned in section III. The information semiring is $<W^I, \ max, min, \mathbf{0}, \mathbf{1}>$ Similarly the communication trust is denoted as $w^C_{kl} \in W^C$ and the communication semiring as $<W^C, \ max, min, \mathbf{0}, \mathbf{1}>$. The trust semiring is defined as $TS =< W^I \times W^C, \ +_{trust}, \times_{trust}, \mathbf{0}, \mathbf{1} >$. Now we pose two different sets of constraints on the semiring.

The first trust semiring with constraints is called information preferred SCSP. As the name suggests, the superior trust relation is information trust. Then the semiring operations are defined as follows. Let (w^I_1, w^C_1) and (w^I_2, w^C_2) be two sets of trust pairs. Then

$$(w^I_1, w^C_1) +_{trust} (w^I_2, w^C_2) = \begin{cases} (w^I_1, w^C_1) & if\ w^I_1 > w^I_2 \\ (w^I_2, w^C_2) & if\ w^I_1 < w^I_2 \\ (w^I_1, \max(w^C_1, w^C_2)) & if\ w^I_1 = w^I_2 \end{cases}$$

$$(w^I_1, w^C_1) \times_{trust} (w^I_2, w^C_2) = (\min(w^I_1, w^I_2), \min(w^C_1, w^C_2))$$

It is trivial to check that indeed the above operations form a *c*-semiring.

The second trust semiring with constraints is called communication preferred SCSP. The communication trust is considered to be superior. Then the semiring operations are defined as follows.

$$(w^I_1, w^C_1) +_{trust} (w^I_2, w^C_2) = \begin{cases} (w^I_1, w^C_1) & if\ w^C_1 > w^C_2 \\ (w^I_2, w^C_2) & if\ w^C_1 < w^C_2 \\ (\max(w^I_1, w^I_2), w^C_1) & if\ w^C_1 = w^C_2 \end{cases}$$

$$(w^I_1, w^C_1) \times_{trust} (w^I_2, w^C_2) = (\min(w^I_1, w^I_2), \min(w^C_1, w^C_2))$$

Again, it is easy to check that the above operations form a *c*-semiring.

This specific trust SCSP actually has a distributed solution where the following algorithm is carried out at every node in the network. At each node, there are semiring elements w_{kl}=

$(w_{kl}^{I}, w_{kl}^{C}), \forall l \in \mathbb{N}_k$. Every node k is assumed to have access to the semiring elements $X_l^n(D), \forall l \in \mathbb{N}_k$, which represents the evaluated trust to target D via a chain of n direct trust relations.

```
**Alogirthm**: The distributed solution to solve the SCSP.
Repeat
    $X_k^{n+1}(D) = \sum_{l \in \mathbb{N}_k} w_{kl} \times_{trust} X_l^n(D)$
Until $X_k^n(D)$ converges.
```

where $\sum = +_{trust}$. Notice that there are only bounded message exchanges in the local neighborhood.

VI. CONCLUSIONS

In this paper, we introduce the valued directed graph with weighted nodes as our model for composite trust. We extend the valued directed graph with weighted nodes composite trust model to include not only numerical weights, but also constraints. We show that the semiring-based constraint satisfaction problem (SCSPs) framework can serve as the unified model to investigate trust relations establishment. It is our plan for future work to apply the trust constraint system to real scenarios and show that our proposed trust model is able to establish trust in highly heterogeneous networked multi-agent systems.

VII. ACKNOWLEDGMENT

Research partially supported by AFOSR MURI award number FA9550-10-1-0573, by AFOSR MURI award number FA9550-09-1-0538, and by ARO MURI award number W911-NF-0710287.

REFERENCES

Agrawal, D., Chivers, H., Clark, J., Jutla, C., & McDermid, J. (2008). A Proposal for Trust Management in Coalition Environments. *Proceedings of ASC 2008.*

Baccelli, F. L., Cohen, G., Olsder, G. J., & Quadrat, J.-P. (1992). *Synchronization and Linearity: An Algebra for Discrete Event Systems* (1st ed.). John Wiley and Sons.

Baras, J. S., & Jiang, T. (2005). Cooperation, Trust and Games in wireless networks. In E. Abed (Ed.), *Proceedings of Symposium on Systems, Control and Networks, honoring Professor P. Varaiya* (pp. 183-202). Birkhause.

Baras, J. S., Jiang, T., & Purkayastha, P. (2008). Constrained Coalitional Games and Networks of Autonomous Agents. *Proceedings of the Third International Symposium on Communications, Control and Signal Processing*, (pp. 972-979). St. Julians, Malta.

Bistarelli, S. (2004). *Semirings for Soft Constraint Solving and Programming, Lecture Notes in Computer Science* (Vol. 2962). Heidelberg: Springer-Verlag, Berlin.

Blaze, M., Feigenbaum, J., & Lacy, J. (1996). Decentralized Trust Management. *Proceedings of 17th Symposium on Security and Privacy* (pp. 164-173). IEEE CS Press.

Bloch, I. (1996). Information combination operators for data fusion: a comparative review with classification. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on , 26* (1), 52-67.

Buskens, V. (2002). *Social Networks and Trust.* Kluwer Academic Publishers.

Chiang, M., Low, S. H., Calderbank, A. R., & Doyle, J. C. (2007). Layering as Optimization Decomposition: A Mathematical Theory of Network Arhitectures. *Proceedings of the IEEE , 95* (1), 255-312.

Gambetta, D. (1988). Can we trust trust? In D. Gambetta (Ed.), *Trust, Making and Breaking Cooperative Relations* (pp. 213-237). Oxford: Basil Blackwell.

Jiang, T., & Baras, J. S. (2008). Trust Credential Distribution in Autonomic Networks. *Proceedings of Globecom.* New Orleans, LA.

Jiang, T., & Baras, J. S. (2006). Trust Evaluation in Anarchy: A Case Study on Autonomous Networks. *Proceedings of the 2006 IEEE INFOCOM.* Barcelona, Spain.

Josang, A. (2001). A Logic for Uncertain Probabilitie. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems , 9* (3), 279-311.

Josang, A., & Ismail, R. (2002). The Beta Reputation System. *Proceedings of the 15th Bled Conference on Electronic Commerce.* Bled, Slovenia.

Kamvar, S. D., Schlosser, M. T., & Garcia-Molina, H. (2003). The EigenTrust Algorithm for Reputation Management in P2P Networks. *Proceedings of the 12th Initernational World Wid Web Conference*, (pp. 640-651). Budapest, Hungary.

Lampson, B., Abadi, M., Burrows, M., & Wobber, E. (1991). Authentication in distributed systems: Theory and practice. *Proceedings of the 13th ACM Symposium on Operating Systems Principles*, (pp. 265-310).

LeBoudec, J. Y., & Thiran, P. (2004). *Network Calculus: A Theory of Deterministic Queueing Systems for the Internet, Lecture Notes in Computer Science* (Vol. 2050). Berlin, Heidelberg: Springer-Verlag.

Maurer, U. (1996). Modelling a Public-Key Infrastructure. *Proceedings of 1996 European Symposium on Research in Computer Security – ESORICS'96*, (pp. 325-350).

Myerson, R. B. (1977). Graphs and Cooperation in Games. *Mathematics of Operations Research, 2*, 225-229.

Russell, S., & Norvig, P. (1995). *Artificial Intelligence: A Modern Approach.* Upper Saddle River, NJ: Prentice Hall.

Slikker, M., & Van den Nouweland, A. (2001). *Social and Economic Networks in Cooperative Game Theory.* Kluwer Academic Publishers.

Sun, Y. L., Han, Z., Yu, W., & Liu, K. J. (2006). A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks. *INFOCOM 2006: Proceedings of 25th IEEE International Conference on Computer Communications.*

Theodorakopoulos, G., & Baras, J. S. (2006). On Trust Models and Trust Evaluation Metrics for Ad-Hoc Networks. *Journal of Selected Areas in Communications, Security in Wireless Ad-Hoc Networks , 24* (2), 318-328.

Zimmermann, P. R. (1995). *The Official PGP User's Guide.* Cambridge, MA: MIT Press.