2013 19th IEEE International Conference on Parallel and Distributed Systems

Trust-based Multi-Objective Optimization for Node-to-Task Assignment in Coalition Networks

Jin-Hee Cho*, Ing-Ray Chen†, Yating Wang†, and Kevin S. Chan*

*U.S. Army Research Laboratory
Computational and Information Sciences Directorate
{jinhee.cho, kevin.s.chan}@us.army.mil

†Virginia Tech
Department of Computer Science
{irchen, yatingw}@vt.edu

***Abstract*—A temporary coalition is often formed to pursue a common goal based on the collaboration of multiple partners who may have their own objectives. The coalition network must attain multiple objectives, under resource constraints and time deadlines. We propose a task assignment algorithm for a scenario where tasks are dynamic, with different arrival times and deadlines. We propose a heuristic coalition formation technique that uses multiple dimensions of trust (i.e., integrity, competence, social connectedness, and reciprocity) to assess trust of each entity. The proposed scheme enables task leaders to make critical assignment decisions based on assessed trustworthiness of entities. We consider three different objectives, namely, maximizing resilience and resource utilization while minimizing delay to task completion. We devise a ranking-based heuristic with linear runtime complexity to select members based on risk derived from trust assessment of nodes. We validate the performance of our proposed scheme by comparing our scheme with a non-trust-based baseline scheme as well as a global optimal solution implemented with the Integer Linear Programming technique.**

Keywords—multi-objective optimization, task assignment, trust, risk

I. INTRODUCTION

Tactical networks deployed to support military missions, disaster management, and/or emergency situations, often require forming a temporary coalition in order to execute a given mission where effective and efficient asset-task assignment is critical to mission success. Under a global objective of completing the mission successfully, the network or system may have multiple objectives to achieve, with participating parties seeking to maximize their own utilities. The multiple objectives in coalition network environments commonly involve high mission performance under resource constraints and required quality-of-service (QoS).

Multi-objective optimization (MOO) problems have been studied extensively in various domains [16]. A common technique is to represent multiple objectives by a single utility (or payoff) function. Since very often multiple objectives tend to be conflicting, the optimal solutions may not be unique. As a result, MOO problems often have a set of *Pareto optimal solutions* referred to as the *Pareto frontier* [8].

Trust is defined differently based on the application domain [2], [4]. However, we find a common definition of trust applicable across domains: willingness to take a risk. Cho et al. [6] discussed the key characteristics of a desirable trust metric in tactical networks in terms of potential risk, context-dependency, dynamicity, and reliability.

In this work, as an extension of [4] which mainly focused on identifying an acceptable risk level to maximize mission completion ratio, we propose a task assignment technique that aims to meet multiple objectives. In [4], the processes of bidding and winner determination may involve nodes' risk behaviors. In this work, the proposed task assignment protocol enables a task leader (TL) to select its members based on risk derived from assessed trustworthiness of nodes with the goal of optimizing multiple objectives. It takes a ranking-based heuristic approach for member selection with linear runtime complexity compared to exhaustive search, without compromising performance. In this work, we consider three system objectives: (1) maximizing mission completion ratio in the presence of hostile or faulty entities (i.e., high resilience to hostility/failure); (2) maximizing utilization of entities in the network, such that each node attempts to maximize its busy time to increase its privileges to access network resources; and (3) minimizing the delay to complete time-sensitive tasks for QoS. Our work aims to identify an optimal solution of multiple task assignments to entities with diverse capabilities/characteristics to meet the multiple objectives. Identifying the optimal set of members for each task team (i.e., the optimal coalition structure in dynamic coalition formation) is the key to solving this problem.

The contributions of this work are summarized as follows. First, to the best of our knowledge, this work is the first to solve a MOO problem dealing with multiple, concurrent and dynamic coalition formations (task assignments) using a composite trust metric based on multiple trust dimensions (i.e., integrity, competence, reciprocity, social connectedness). Second, this work proposes and analyzes a new design concept of trust-based MOO by computing risk based on assessed trust levels to screen task team members for node-to-task assignment. Third, the three objectives considered in the paper

1521-9097/13 $31.00 © 2013 IEEE
DOI 10.1109/.58

preserve both individual welfare in terms of maximizing utilization, and global welfare in terms of maximizing mission completion ratio and minimizing extra delay to task completion. Last, we perform a comparative analysis of our proposed heuristic ranking-based member selection strategy with both a non-trust baseline scheme through simulation study as well as an optimal solution implemented with the Integer Linear Programming (ILP) technique, to demonstrate the effectiveness of our approach.

The rest of this paper is organized as follows. Section II gives an overview of existing MOO research. Section III describes our system model including the network, node/task models, trust metrics, and our MOO problem definition. Section IV describes the proposed MOO task assignment protocol. Section V formulates the task assignment problem as an ILP problem, and proposes a low-complexity rank-based heuristic scheme. Section VI presents a comparative analysis of the ILP-based optimal solution against those generated from our proposed ranking-based member selection heuristic scheme and a non-trust baseline scheme, with physical interpretations given for the general trends observed. Section VII concludes the paper.

II. Related Work

In this section, we discuss related work in terms of coalition formations, task assignment, or team formation. In particular, we focus on how trust is used to solve MOO problems. We categorize existing work on MOO into three classes based on global welfare (system objectives) vs. individual welfare (individual objectives): (1) global welfare only; (2) both global welfare and individual welfare are considered and the individual payoff function is the same for all agents in the system; and (3) both global welfare and individual welfare are considered and agents have different individual payoff functions. The MOO problem considered in this work belongs to Class 2 (C2).

Class 1 (C1) MOO problems deal with only multiple system/network objectives for global welfare [9], [10], [11].

A dynamic trust computation model was proposed in [9] to detect malicious nodes while achieving load balance among agents. A MOO problem was investigated in [10] with the objectives of minimizing energy consumption and data volume while maximizing QoS in a large wireless sensor network. A team formation problem with the objectives of maximum skill coverage and high team connectivity was studied in [11].

Class 2 (C2) MOO problems are for applications with both global welfare and individual welfare where the individual payoff function is the same for all agents [4], [13], [18].

A trust-based task assignment protocol was proposed in [4] to select team members to maximize the mission completion ratio while meeting an acceptable risk level. A trust and motivation based clan formation method was studied in [13]. Here, self-interested agents want to maximize their payoff by joining, maintaining, or dissolving a clan while a coalition aims to maximize its payoff with minimum overhead. An agent-to-task allocation for coalition formation in wireless networks was investigated in [18] using hedonic game theory in order to maximize throughput while minimizing the mean delay for task execution. In C2 MOO research, we observe that the goal of an individual entity and that of a coalition are well aligned and mutually beneficial to maximize their payoffs.

Class 3 (C3) MOO problems are for applications with both global welfare and individual welfare, but the individual payoff functions are different, distinct from Class 2. A long-term vendor-customer coalition formation problem was studied in [1]. This work measured trust based on positive experience in transactions and similarity in preferences. A mathematical approach to modeling MOO problems using game theory was presented in [17].

Among the literature cited above, [1], [4], [9], [11], [13] studied coalition (or team, clan, alliance) formation or task assignment using trust to solve the MOO problem. However, except our prior work [4], these prior works assume that trust is already in place and can be used as a metric to help achieve MOO. Different from the existing work, this work proposes a trust-based task assignment protocol to solve a C2 MOO problem in tactical coalition networks. In our model, trust assessment is dynamically performed by each node in a distributed manner, operating in a hostile network environment.

III. System Model

A. Node Model

Nodes may be heterogeneous with vastly different functionalities and natures. For example, the entities may be sensors, robots, unmanned vehicles or other devices, dismounted soldiers or first response personnel carrying sensors or handheld devices, and manned vehicles with various types of equipment. We consider M node types, NT_1, …, NT_M, ordered such that a higher node type has more capability than a lower node type. A node with a higher node type involving human also has more trust dimensions than a node with a lower type node. When nodes are not involved in a task, they follow a random mobility model, characterized by node-specific speed v_i. Each node can monitor its neighboring nodes, with detection error specified by false positive and false negative probabilities (i.e., P_i^{fp}, P_i^{fn}). Nodes may be malicious, i.e., exhibit behaviors such as message modification or forgery, and dissemination of fake information via bad mouthing to destroy a node's reputation or good mouthing for ballot stuffing. Nodes that always exhibit such behaviors will be easily detected through the trust assessment; hence we model the behavior probabilistically. Our trust metric, discussed next, captures various behavioral aspects of a node.

B. Trust Metric

We use a composite trust metric proposed in our prior work [7]. We consider four trust dimensions in this work: social connectedness, reciprocity, competence, and integrity. We select these four dimensions with the following reasons: (1) social connectedness enhances connectivity and productivity by sharing information and resources; (2) reciprocity ensures reliable and consistent service provision based on past trust relationships; (3) competence guarantees a certain level of availability and willingness to respond to received requests;

and (4) integrity protects the task from misbehaving nodes that do not comply with network protocols. In our work, nodes of type NT_1 and NT_2 are evaluated based on only competence and integrity assuming that nodes are machines; nodes of type NT_3 and NT_4 are evaluated on all four trust dimensions. Other trust dimensions can be considered depending on task characteristics. Our trust protocol is generic and can incorporate other trust dimensions easily. We discuss each trust component in the following:

- **Social Connectedness (SC)**: We compute this as the number of nodes each entity encounters during a certain time period, being affected by mobility and inherent sociability. We assume that each node sends out an encounter history certified by encounter tickets [5], [6], [14] to its 1-hop neighbors. This enables each node to know the level of social connectedness of its 1-hop neighbors (i.e., T_i^{SC}).
- **Reciprocity (R)**: This is the degree of mutual giving and receiving based on the inherent willingness to reciprocate. Each node counts a target node's reciprocity based on the frequency of receiving events (e.g., receiving the result of a query) from a target node over the total number of giving actions (e.g., providing requested services) to the target node (i.e., T_i^R).
- **Competence (C)**: This refers to an entity's capability to serve the received request, being affected by: (a) unintentional unavailability due to network conditions (i.e., link unreliability); and (b) intentional nature of an entity such as willingness to serve. This is modeled probabilistically by the probability of competence (T_i^C). Each node measures its 1-hop neighbors' behaviors based on the frequency of positive behaviors over total experiences in packet forwarding behavior.
- **Integrity (I)**: This is the degree of honesty of an entity based on the number of positive experiences over the total number of experiences in terms of network behaviors. We compute this as T_i^I the frequency of positive behaviors (i.e., not performing any network attacks considered in this work) over total experiences in complying with a given network protocol.

For this paper to be self-contained, we briefly describe the trust metric used in this work. Let $T_j^X(t)$ denote the objective trustworthiness of node j on component X at time t. $T_{i,j}^X(t)$ is node i's evaluation of $T_j^X(t)$. Trust values lie in [0, 1] where 1 indicates complete trust, 0.5 ignorance, and 0 distrust. Trust estimates are updated every Δt seconds as a combination of direct and indirect evidences as:

$$T_{i,j}^X(t) = \alpha T_{i,j}^{D-X}(t) + (1-\alpha) T_{i,j}^{ID-X}(t) \quad (1)$$

where α is a weight factor that lies in [0,1] and X=SC, R, C, or I. $T_{i,j}^{D-X}(t)$, is the direct trust of node i toward node j on X based on node i's direct observations of node j during that time interval. $T_{i,j}^{D-X}(t)$ is to be assessed by node i toward node j as described earlier. The direct observations are subject to detection errors (i.e., false positive/negative probabilities). $T_{i,j}^{ID-X}(t)$ is the indirect trust which is computed by the average of valid recommendations (trust values) received in that interval. If no fresh evidence is available, the trust component is merely the discounted prior estimate, $\gamma T_{i,j}^X(t - \Delta t)$, where the decay factor γ lies in [0, 1]. In this trust metric, we fine-tune the experimental setting to maximize trust accuracy by using a set of optimal parameters including the range of hops (i.e., called the "trust chain length" denoted by L_{TC}) to receive recommendations (indirect evidence), trust decay (γ), and the weights for direct/indirect evidences (α and 1- α). Refer to [7] for more details on the trust metric used in this work. In this paper, we use the assessed trust values to derive risk. Specifically, risk derived from trust is used as the basis of member selection for task execution. Since accurate trust assessment is critical to correctly measuring risk which significantly impacts member selection decisions, we apply the optimal trust parameter setting (i.e., α, γ, and L_{TC}) identified in [7] to minimize the discrepancy between measured trust (i.e., $T_{i,j}^X(t)$) and actual trust (i.e., $T_j^X(t)$).

C. Network Model

We consider a mission-oriented tactical network where stationary (i.e., sensors) and/or mobile nodes communicate through multiple hops. We adopt a hierarchical structure to execute a mission consisting of multiple tasks (described in Section II.D). A commander node (CN) governs the mission team. Under the CN, multiple task leaders (TLs) lead task teams. The CN selects TLs at the beginning of network deployment based on the trustworthiness of nodes known to CN a priori and the TLs recruit regular members (RMs) for task execution based on periodic dynamic trust assessment. A group key is used for communications among members to prevent outside attackers.

D. Task Model

Tasks arrive asynchronously and may start and end at different times. We denote the start time, end time and duration of task m by T_m^{start}, T_m^{end} and DT_m. Each task has unique properties:

- *Required node type* NT_m indicates the required functionality of nodes for executing task m. A node with a higher node type has a higher capability and, because of human involvement, also has more trust dimensions.
- *Required number of nodes* N_m refers to the number of nodes needed for execution of task m.
- *Minimum trust threshold* T_m^{X-th} is a threshold for each trust property X of task m.
- *Importance* (I_m) refers to the impact of task failure on mission completion with higher values indicating more importance.
- *Urgency* (UR_m) indicates how urgently a given task should be completed where higher is more urgent. Less urgent tasks may be allowed extra time for completion, beyond the nominal end time. A task is regarded as successful if it is completed within its deadline, defined by:

$$T_m^{deadline} = T_m^{end} + \left(DT_{mission} - T_m^{end}\right)\left(\frac{UR_{max} - UR_m}{UR_{max}}\right) \quad (2)$$

$DT_{mission}$ is the mission duration and UR_{max} is the maximum urgency level.

- *Difficulty* (DF_m) represents the degree of a task's difficulty that is modeled associated with the competence trust threshold per task as shown in Table III (Section VI).

E. System Objectives

A CN aims to achieve the system goal in terms of three objectives: *mission completion ratio*, *resource utilization*, and *delay of task completion*.

- **Mission Completion Ratio (P_{MC}):** This is the fraction of the sum of completed tasks weighted by respective importance over the sum of all tasks' importance values, and is computed by:

$$P_{MC} = \sum_{m \in L_c} \frac{I_m}{\sum_{all} I_m} \quad (3)$$

  L is the set of mission tasks, and L_c is the set of completed tasks. Higher P_{MC} is desirable.
- **Resource Utilization (U):** This measures the average utilization of nodes and is defined by:

$$U = \frac{\sum_{i \in N} U_i}{|N|} \text{ where } U_i = \sum_{m \in L} U_{i,m} \quad (4)$$

  N is the set of legitimate member nodes. $U_{i,m}$ equals $DT_m/DT_{mission}$ if node i executes task m, and is zero otherwise. Higher U is desirable (minimizing idle time).
- **Delay to Task Completion (D):** This is the average extra fractional delay for task completion, defined by:

$$D = \frac{\sum_{m \in L} D_m}{|L|} \text{ where } D_m = \frac{\left(T_m^{complete} - T_m^{end}\right)}{DT_m} \quad (5)$$

  $T_m^{complete}$ is the actual completion time of task m which must happen before $T_m^{deadline}$. If a task is not completed by $T_m^{deadline}$ (i.e., task m fails), $T_m^{complete}$ is set to $T_m^{deadline}$. Lower D is desirable.

The MOO problem we are solving here is to maximize P_{MC} and U and to minimize D via node-to-task assignment, given node and task characteristics as input. A well-accepted way of dealing with multiple objectives is to optimize a linear combination, such as:

$$P_{MOO} = P_{MC} + U - D \quad (6)$$

Each node may participate only in one task at a given time. In practice, all tasks will not be known in advance, and the task allocation process must proceed, taking into account currently available resources.

IV. Task Assignment Protocol

We have two layers of task assignment: by CN to TLs and by TLs to RMs. For simplicity of exposition and due to space limitations, we assume that the CN-to-TL assignment has already been done based on prior trust profiles of the nodes. A TL is involved in only one task at a time, and a node can participate in only one task at a time, although it may participate in multiple tasks during its lifetime. TLs advertise tasks and free nodes respond as described next.

A. Advertisement of Task Specification

The task specification disseminated during the auction process includes a set of requirements for task execution specified by:

$$\left[ID_m, I_m, NT_m, (T_m^{start}, T_m^{end})\right] \quad (7)$$

ID_m is the identifier of task m. A node meeting the node type requirement NT_m is considered capable of handling the required work elements imposed by task m and will respond to the request with its node ID if it is free. A node may respond to only one task advertisement at a time.

An individual node aims to maximize its privilege to access network resources by maintaining its trusted status as a member of the mission team. The payoff considers not only the busy time for executing a task (i.e., utilization), but also the task importance and the role of a node (i.e., a TL role gives a higher role score than a RM). Specifically, the payoff to node i for executing task m is calculated as:

$$PO_{i,m} = RRS_i \times I_m \times \frac{DT_m}{DT_{mission}} \quad (8)$$

where RRS_i is the Role-based Reward Score. $PO_{i,m}$ is used in computing a trust reward or penalty as discussed Equation 11. If multiple task requests are pending, a node would respond to the task that offers the highest immediate payoff.

B. Member Selection

The inclusion of node j in task m involves a risk which we model, following Lund et al. [15], as

$$r_{m,j}(t) = UR_m \frac{\sum_{X \in T} r_{m,j}^X(t)}{|T|} \text{ where } r_{m,j}^X(t) = e^{-\rho \frac{T_{i(m),j}^X(t)}{T_m^{X-th}}} \quad (9)$$

Here i(m), the evaluator of node i's trustworthiness, is the task leader of task m. The lower the estimated trust, relative to the task's threshold trust, the larger is the risk. Note that even with perfect trust (=1), risk is non-zero, reflecting that risk cannot be removed perfectly even under very high trust [15]. ρ is a positive-valued design parameter. We model that risk is linear in urgency but exponential in the trust factor.

TLs implicitly seek to optimize the MOO function. However, TLs work independent of one another. As such they can only adopt heuristics. The TL of task m ranks all responding nodes based on the risk level, $r_{m,i}(t)$, that node i exposes in executing task m. TL selects the N_m nodes with the lowest rank of the risk level for task execution. The idea is to select members with low risk so as to have a chance to maximize the MOO function defined in Equation 6. Among all objectives, the mission completion ratio is highly sensitive to exposed risk; it also dominates the other two objectives (utilization and delay) in the MOO function, thereby affecting the performance of utilization and delay. A selected node commits itself to the assigned task.

If sufficient members are not found, TL can re-advertise the task at the next trust update interval when the node's trust values are updated, assuming that the task can be scheduled to execute to completion before $T_m^{deadline}$. Otherwise, the task is assumed to have failed.

C. Task Failure

A task fails if it cannot be successfully completed by its deadline. As indicated earlier, a task may fail simply because an appropriate team could not be formed. A task may also fail if the team has too many untrustworthy nodes, i.e., with trust levels below the required trust thresholds: Failure occurs if

$$\frac{\sum_{j\in m} F_j(t)}{N_m} > TH_m$$
$$\text{where } F_j(t) = \begin{cases} 1 & \text{if } T_j^X(t) \le T_m^{X-th} \text{ for any X} \\ 0 & \text{otherwise} \end{cases} \quad (10)$$

Here TH_m indicates the tolerance level of task m to untrustworthy nodes, and $T_j^X(t)$ denotes the objective trust. If a TL detects task failure, then it re-advertises the task and triggers task reassignment following the procedure described in Section IV.B, with the task being rescheduled as a new task to be completed within $T_m^{deadline}$.

D. Trust Reward and Penalty

Since an individual node aims to maximize its privilege to access network resources by maintaining a sufficiently high trust level in the network, receiving or deducting a trust value can be an effective reward or penalty to the individual node. A node will receive a trust reward or penalty based on the result of task completion or failure via positive or negative recommendations as trust is being updated. The reward or penalty function is:

$$M_{reward}^{m,j}(t) = M_{penalty}^{m,j}(t) = \frac{PO_{j,m}}{T_{i,j}(t)} \quad (11)$$

where node i is the TL of task m, $PO_{j,m}$ is the individual payoff of node j when it executes task m as given in Equation 7. Notice that less trusted nodes get higher penalties and rewards compared with more trusted nodes.

V. The Task Assignment Problem

The node-task optimization problem to maximize P_{MOO} is combinatorial and NP-complete [12]. This means that the optimization problem is not polynomially solvable in runtime with respect to the number of bidders (N_B), resulting in a lower bound approximation of $\omega(2^{N_B})$.

Suppose that all tasks are known a priori – what is the best possible performance? We can formulate this as ILP problem [1] which searches for the best solution that satisfies the constraints and maximizes P_{MOO} for node-to-task assignment. Different from Section IV, this section gives theoretical validation of identifying optimal solutions against which the proposed trust-based and non-trust-based protocols (shown in the end of this section) are compared. Here we note that the solutions by the non-trust-based and ranking-based schemes reflect network/trust dynamics, but ILP-based optimal solutions may not. However, the ILP-based optimal solution is a benchmark to prove the benefit of the trust-based heuristic approach with much less complexity.

Table I defines the variables used in the ILP formulation. There are three types of variables. The input variables summarize the task/node specifications given as input to the ILP. There is only one decision variable, namely, $w_{j,m}$ to be determined by the ILP, specifying if node j should be assigned to task m. The ILP will search for an optimal solution of $w_{j,m}$ for all j, m's to maximize $P_{MOO} = P_{MC} + U - D$. The objective variables P_{MC}, U, and D have the same meanings as discussed before, each now being defined in Table I as a linear function of $w_{j,m}$ (the only decision variable to be decided by the ILP).

TABLE I. Variable definitions for ILP

Type	Variable	Definition
input	$o_{p,q}$	1 if task p and task q are overlapping in time; 0 otherwise
input	O	Union of set {p, q} for which $O_{p,q}$ =1
input	$t_{j,m}$	1 if $T_j^X \ge T_m^X$ for every trust property X over the task execution period; 0 otherwise
input	$nt_{j,m}$	1 if node j's node type satisfies the required node type of task m; 0 otherwise
decision	$w_{j,m}$	1 if node j is assigned to task m; 0 otherwise
objective	$P_m^{complete}$	$\sum_j (t_{j,m} \times w_{j,m}) / N_m$
objective	P_{MC}	$P_{MC} = \sum_{m\in L_c} \frac{I_m}{\sum_{all} I_m}$
objective	U	$\sum_m \left(\sum_j t_{j,m} \times w_{j,m} \right) \times U_m / \lvert N \rvert$
objective	D_m	$(1 - P_m^{complete}) \times \left(T_m^{deadline} - T_m^{end} \right) / DT_m$
objective	D	$\frac{\sum_{m\in L} D_m}{\lvert L \rvert}$
objective	P_{MOO}	$P_{MC} + U - D$

The task assignment optimization problem is formulated as follows:

Given: $L, N, O, o_{p,q}, t_{j,m}, nt_{j,m}$

Find: $w_{j,m} \in \{0, 1\}$

Maximize: $P_{MOO} = P_{MC} + U - D$

Subject to: $\forall j \; \forall \{p, q\} \in O, \; w_{j,p} + w_{j,q} \le 1; \; \sum_j w_{j,m} = N_m; \; w_{j,m} \le nt_{j,m}$.

The task/node specifications including the task requirement and arrival sequence, as well as the node trust and risk behaviors are summarized by the set of variables defined under "given: $L, N, O, o_{p,q}, t_{j,m}, nt_{j,m}$." Specifically, L is the set of tasks; N is the set of nodes; O is the set of pairs of concurrent tasks for which $o_{p,q}$ =1; $t_{j,m}$ and $nt_{j,m}$ are input specifying if node j satisfies task m's trustworthiness requirement and node type requirement, respectively. The ILP will try all possible combinations of $w_{j,m}$ for all j, m's such that $P_{MOO} = P_{MC} + U - D$ is maximized. Under "subject to" we list the constraints that must be satisfied by a solution found by the ILP. The first constraint specifies that for any two concurrent tasks, a node can only be assigned to one of them for execution. However, a node needs not at all be assigned to either task. The second constraint specifies that the

required number of qualified nodes must be assigned to task m. The third constraint specifies that a node assigned to task m must be of the required type or higher (more capable).

We propose two member selection strategies to cope with the complexity of ILP and the asynchronous task arrival pattern:

- *Non-trust-based selection*: TLs do not use any trust/risk analysis to select members. The TL of task m selects N_m members *randomly* among all bidders with qualified node type.
- *Ranking-based selection*: TLs select members based on trust-based risk analysis discussed in Section IV.B. Top N_m nodes with the lowest risk are selected as members.

These two schemes will be compared against the ILP solution to demonstrate the ranking-based member selection strategy approaches the optimal solution achieved by the ILP without high complexity.

VI. Numerical Results and Analysis

In this section, we compare the performance of the three team member selection strategies by a TL. Our case study is for a small size problem with 5 tasks and 40 nodes where $DT_{mission}$ is 12 hrs and the square-shaped operational area is 1000m×1000m. Nodes communicate within wireless radio range of 250 m. Table II summarizes other key default values used for this case study. The trust thresholds for T_m^{I-th}, T_m^{R-th}, and T_m^{SC-th} and detection error probabilities (i.e., P_i^{fp} and P_i^{fn}) are randomly selected based on uniform distribution from the ranges shown in Table II. Table III summarizes the ranges of the competence trust threshold, T_m^{C-th}, according to the level of task difficulty (DF_m), as discussed earlier in Section III.D.

TABLE II. Key parameters and default values

Parameter	Value	Parameter	Value	Parameter	Value
TH_m	1/3	$\|L\|/N_m$	5 / 4	L_{TC}	4
DT_m	2 hrs	α / γ	0.1 / 0.95	T_m^{R-th}	[0.5, 0.9]
c	1.3	Δt	5 min.	T_m^{SC-th}	
ρ	7	P_i^{fp}, P_i^{fn}	(0, 0.01]	T_m^{I-th}	[0.8, 0.9]

TABLE III. Task difficulty and competence threshold per task T_M^{C-TH}

DF_m	1	2	3	4	5
T_m^{C-th}	[0.4, 0.5]	[0.5, 0.6]	[0.6-0.7]	[0.7, 0.8]	[0.8, 0.9]

In the results shown in this section, each result point indicates the average value of the metric based on 100 simulation runs; error bars depict the standard deviations. We maintain less than 3~8% difference between measured trust (i.e., $T_{i,j}^X$) and actual trust (i.e., T_i^X), given a wide range of original trust seeds (i.e., [0.5, 1] to [0.8, 1]), to avoid prediction inaccuracy. This is achieved by using the optimal setting identified (i.e., the trust chain length L_{TC} = 4, α = 0.1, and γ = 0.95) to minimize trust bias as discussed in Section IV.A. P_{MOO} is calculated based on Equation 6 but is scaled such that $P_{MOO} > 0$ (i.e., $P_{MOO} + 1$).

We first report numerical results (in Figs. 1-4) for a small size problem solvable by optimal selection through ILP so we can compare performance of ranking-based selection and non-trust-based selection (random selection) against optimal solution. Then with a large size problem (i.e., more tasks/nodes), we report performance comparison results (in Figs. 5-7) of ranking-based selection against non-trust-based selection, and perform sensitivity analysis of the results with respect to trust bias, the number of tasks, and the number of nodes in the system.

Figs. 1-4 show performance comparison results of mission completion ratio (P_{MC}), utilization (U), delay (D), and P_{MOO} (Equations 3-6), respectively. The X-coordinate indicates the range of trust in terms of [P_{GB}, 1] where P_{GB} is the lower trust bound, with a larger P_{GB} close to 1 representing a more trustworthy environment.

Fig. 1 compares the three team member selection strategies in mission completion factor (P_{MC}). As expected, the optimal selection by the ILP performs the best at the expense of high computational complexity.

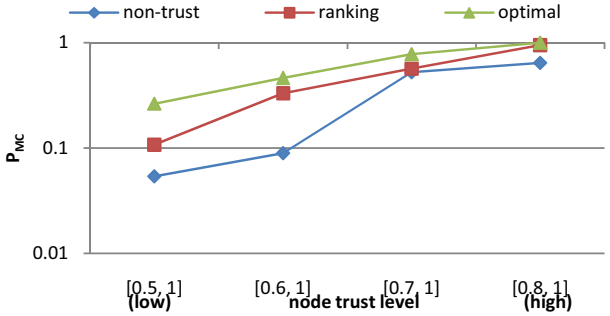

Fig. 1: Comparison of three schemes in mission completion ratio (P_{MC})

Ranking-based selection clearly outperforms non-trust-based selection because it can use trust to heuristically select trustworthy nodes with low risk. The main reason for the discrepancy between optimal selection and ranking-based selection is that optimal selection exhaustively considers all possible combinations of task teams that can maximize the overall MOO performance. Nevertheless, we observe that ranking based selection performs comparably over all trust ranges and approaches the optimal ILP solution as the environment becomes more trustworthy (toward right) because of a lower task failure probability.

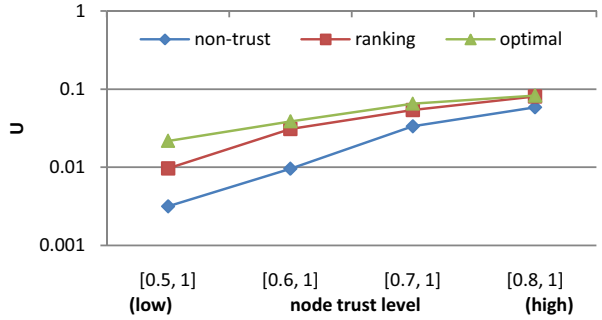

Fig. 2: Comparison of three schemes in utilization (U)

Fig. 2 compares the performance of the three member selection schemes in node utilization (U). Fig. 2 is well matched with Fig. 1, showing that the scheme with higher mission completion ratio also reaches higher utilization. Again, whereas the optimal solution by ILP gives the best

performance, ranking-based selection clearly outperforms non-trust-based selection, and, with only linear complexity, performs comparably to the optimal ILP solution.

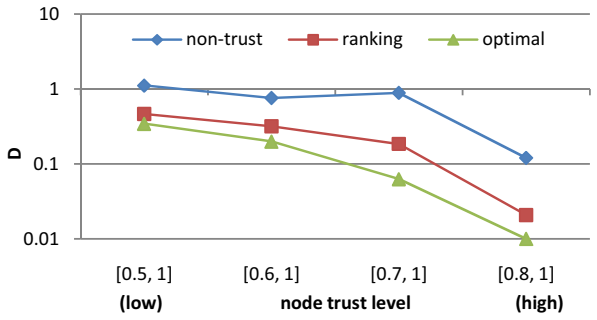

Fig. 3: Comparison of three schemes in delay (D)

Fig. 3 depicts the delay metric. Low delay is desirable. In Fig. 3, the ILP optimal selection has the smallest delay (The optimal solution under [0.8, 1] is not shown because the delay was zero), followed by ranking-based selection and then by non-trust-based selection. The trend correlates well with that of Fig. 1, as delay is inversely correlated to mission completion ratio. However, delay is also affected by deadline extension based on task urgency. Therefore, it is possible that there may be a longer delay when more tasks with extended deadlines are successfully completed. For example, when a task with no deadline extension fails, the delay is zero; when a task with a deadline extension is completed, delay is introduced due to the task reassignment procedure. Therefore, the non-trust-based scheme under the trust range of [0.7, 1] (more trustworthy) shows a slightly higher delay, compared to the delay under the trust range of [0.6, 1] (in a less trustworthy environment).

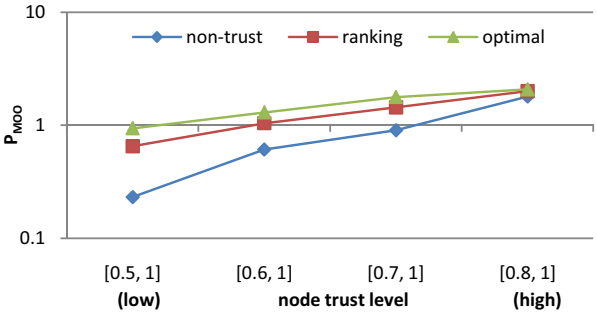

Fig. 4: Comparison of three schemes in MOO function value (P_{MOO})

In Fig. 4, we compare performance in terms of the MOO function value (P_{MOO}). As expected, while optimal selection performs the best, ranking-based selection performs comparably and it significantly outperforms non-trust-based selection particularly when the environment is less trustworthy. This result makes it a feasible runtime solution as the computational complexity is only linear.

Fig. 5 shows how trust bias (expressed in terms of the TC length used) affects P_{MOO}. For ranking-based selection, we see that when the TC is shorter and thus trust bias is higher [7], a lower P_{MOO} is observed. This is because when trust bias is high, ranking based selection may mistakenly take untrustworthy nodes as trustworthy, thus causing tasks to be aborted.

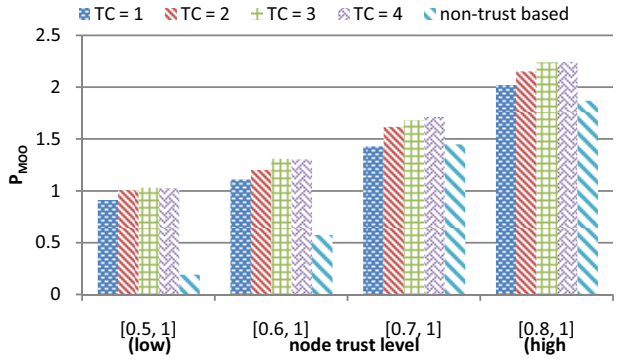

Fig. 5: P_{MOO} of non-trust-based selection vs. ranking-based selection with respect to the length of a trust chain (TC)

This is especially the case when the environment is relatively trustworthy (e.g., when the hostility is in [0.7, 1]) so that the trust value of an untrustworthy node j is just below the minimum trust threshold value (thus satisfying $F_j(t)$ in Equation 10) but because of high trust bias, the trust value of node j is mistakenly considered to be higher than the minimum trust threshold. We see that in this rare condition (TC=1 and hostility is in [0.7, 1]), non-trust-based selection (random selection) can perform comparable to ranking-based selection. In all other cases, ranking-based selection outperforms non-trust-based selection. The robustness of ranking-based selection with respect to trust bias is evidenced by the result that it outperforms non-trust-based selection when trust bias is high (TC=1) and the environment is not trustworthy (e.g., when the hostility is in [0.5, 1]).

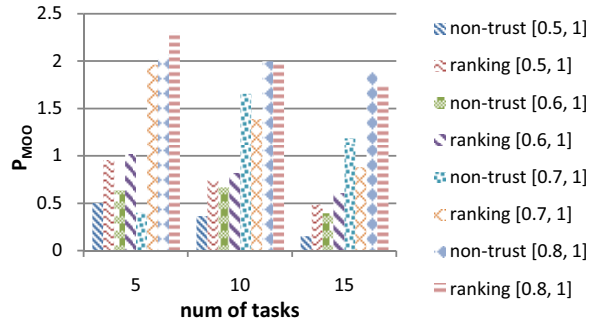

Fig. 6: P_{MOO} of non-trust-based selection vs. ranking-based selection with respect to a different number of tasks (N_m)

Fig. 6 compares MOO performance (P_{MOO}) of ranking-based selection against non-trust-based selection as the number of tasks (N_m) varies in the range of [5, 15] under four different network hostilities. In this experiment, 60 nodes are used given that we have up to 15 tasks each requiring 4 nodes. We observe that ranking-based selection is less effective than non-trust-based selection, when there are more tasks (e.g., 10-15), particularly if the environment is relatively trustworthy (e.g., hostility is in the range of [0.7/0.8, 1]). In ranking-based selection, a TL selects the best nodes based on low risk and

low utilization criteria among all the nodes available in the network. Due to this reason, the order a task arrives is critical for the TL to select best qualified nodes particularly where there are more than one task that require the same node type. In this competing situation, if a task arrives earlier than the other competing task(s), it will have a higher chance to obtain qualified nodes regardless of the importance given to the task. Therefore, in ranking-based selection, overly qualified nodes may be assigned to less important tasks which do not necessary require highly trustworthy nodes. However, in less competing situations with fewer tasks and less trustworthy environments, ranking-based selection significantly outperforms non-trust-based selection.

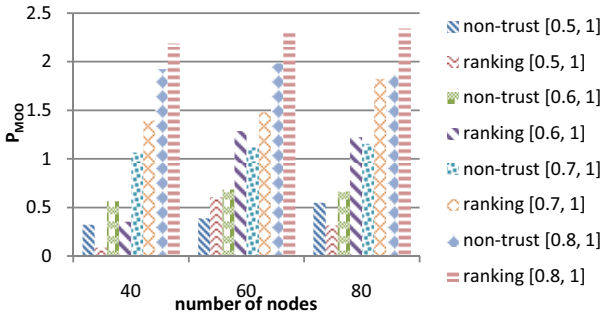

Fig. 7: P_{MOO} of non-trust-based selection vs. ranking-based selection with respect to a different number of nodes (N)

Fig. 7 compares MOO performance (P_{MOO}) of ranking-based selection against non-trust-based selection as the number of nodes (N) varies in the range of [40, 80] under four different network hostilities. We use 10 tasks to create a competing situation in which more than one task may recruit nodes of the same node type. As shown in Fig. 7, compared to non-trust-based selection, ranking-based selection can greatly benefit from having more available nodes in a relatively trustworthy environment (e.g., when the hostility is in the range of [0.7/0.8, 1]). The reason is that ranking-based selection can better exploit abundance of trustworthy nodes to match the required node trust level for task execution, ultimately leading to high mission success rate, low task delay and high utilization, and, consequently, high MOO performance.

VII. CONCLUSION

We proposed a trust-based task assignment protocol for a tactical coalition network where we are concerned with multi-objective optimization (MOO). We developed a ranking-based member selection scheme which trades off complexity for performance. The results demonstrate that our scheme has low complexity and yet can achieve performance comparable to that of the optimal solution by ILP and can significantly outperform random selection. In the future, we plan to refine our heuristic design for member bidding and selection strategies to further enhance MOO performance. We also plan to explore other forms of MOO formulation applicable to other tactical mission scenarios.

ACKNOWLEDGMENTS

This work is supported in part by the U. S. Army Research Laboratory and the U. S. Army Research Office under contract number W911NF-12-1-0445. This research was also partially supported by the Department of Defense (DoD) through the office of the Assistant Secretary of Defense for Research and Engineering (ASD (R&E)). The views and opinions of the author(s) do not reflect those of the DoD or ASD (R&E).

REFERENCES

[1] R.K. Ahuja, T.L. Magnanti, and J.B. Orlin, *Network Flows: Theory, Algorithms, and Applications*. Prentice Hall, Feb. 1993.

[2] F. Bao, I.R. Chen, M. Chang, and J.H. Cho, "Hierarchical trust management for wireless sensor networks and its application to trust-based routing and intrusion detection," *IEEE Trans. on Network and Service Management*, vol. 9, no. 2, pp. 169-183, 2012.

[3] S. Breban and J. Vassileva, "Using inter-agent trust relationships for efficient coalition formation," *15th Conf. of the Canadian Society for Computational Studies of Intelligence on Advances in Artificial Intelligence*, Calgary, Canada, pp. 221-236, May 2002.

[4] M. Chang, J.H. Cho, I.R. Chen, K. Chan, and A. Swami, "Trust-based task assignment in military tactical networks," *17th Int'l Command and Control Research and Technology Symposium*, Fairfax, VA, June 2012.

[5] I. R. Chen, F. Bao, M. Chang, and J. H. Cho, "Trust management for encounter-based routing in delay tolerant networks," *IEEE Global Communications Conf.*, pp. 1-6, Miami, Florida, USA, Dec. 2010.

[6] I.R. Chen, F. Bao, M. Chang, and J.H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Trans. on Parallel and Distributed Systems*, 2013.

[7] J.H. Cho, A. Swami, and I.R. Chen, "Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1001-1012, May 2012.

[8] C. A. C. Coello, "An updated survey of GA-based multiobjective optimization techniques," *ACM Computing Surveys*, vol. 32, no. 2, pp. 109-143, June 2000.

[9] A. Das, and M. M. Islam, "SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems," *IEEE Trans. on Dependable and Secure Computing*, vol. 9, no. 2, pp. 261-274, March/April 2012.

[10] B. Dieber, C. Micheloni, and B. Rinner, "Resource-aware coverage and task assignment in visual sensor networks," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 21, no. 10, pp. 1424-1437, Oct. 2011.

[11] C. Dorn, F. Skopik, D. Schall, and S. Dustdar, "Interaction mining and skill-dependent recommendations for multi-objective team composition," *Data Knowledge Engineering*, vol. 70, no. 10, pp. 866–891, Oct. 2011.

[12] M. R. Garey and D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W.H. Freeman & Co., 1979.

[13] N. Griffiths and M. Luck, "Coalition formation through motivation and trust," *Proc. 2nd Int'l Joint Conf. on Autonomous Agents and Multiagent Systems*, Melbourne, Australia, pp. 17-24, July 2003.

[14] F. Li, J. Wu, and A. Srinivasan, "Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets," *IEEE INFOCOM*, pp. 2428-2436, Rio de Janeiro, Brazil , April 2009.

[15] M. S. Lund, B. Solhaug, and K. Stolen, "Evolution in relation to risk and trust management," *Computer*, vol. 43, no. 5, pp. 49-55, May 2010.

[16] R. T. Marler and J. S. Arora, "Survey of multi-objective optimization methods for engineering," *Structure Multidisc Optimization*, vol. 26, no. 6, pp. 369-395, April 2004.

[17] R. Meng, Y. Ye, and N. G. Xie, "Multi-objective optimization design methods based on game theory," *8th World Congress on Intelligent Control and Automation*, pp. 2220-2227, 2010.

[18] W. Saad, Z. Han, T. Basar, M. Debbah, A. Hjorungnes, "Hedonic coalition formation for distributed task allocation among wireless agents," *IEEE Trans. on Mobile Computing*, vol. 10, no. 9, 2011, pp. 1327-1344.